Image 7.0.X for Chip PC Thin-Clients

User Manual

Document Version 1.0

COPYRIGHT NOTICE

© 2013 Chip PC Inc., Chip PC (Israel) Ltd., Chip PC (UK) Ltd., Chip PC GmbH
All rights reserved.

This product and/or associated software are protected by copyright, international treaties and various patents.

This manual and the software, firmware and/or hardware described in it are copyrighted. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, any part of this publication without express written permission from Chip PC.

CHIP PC SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

The information contained in this document represents the current view of Chip PC on the issues discussed as of the date of publication. Because Chip PC must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Chip PC, and Chip PC cannot guarantee the accuracy of any information presented after the date of publication.

This Guide is for informational purposes only. CHIP PC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

TRADEMARKS

Chip PC, Xcalibur, Xtreme PC, Jack PC, and the Chip PC logo are either trademarks or registered trademarks of Chip PC.

Products mentioned in this document may be registered trademarks or trademarks of their respective owners

The Energy Star emblem does not represent endorsement of any product or service.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software and documentation are provided with RESTRICTED RIGHTS.

You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments.

The information and specifications in this document are subject to change without prior notice.

Images are for demonstration purposes only.

Table of Contents

CHAPTER 1 PREFACE 7

INTENDED AUDIENCE 7
SCOPE 7
OBJECTIVES 7
PREREQUISITES 7
REFERENCE MATERIALS 7

CHAPTER 2 INTRODUCTION TO IMAGE 7.0.X 9

GENERAL 9
PLUG-INS 9
1 Advantages to Using Plug-ins 9
IMAGE 7.0 BOOT SEQUENCE 10

CHAPTER 3 DESKTOP INTERFACE FEATURES 11

OBJECTIVES 11
GENERAL 11
DESKTOP INTERFACE FEATURES 12
DESKTOP INTERFACE ADVANTAGES 13
1 User Friendliness and Familiarity 13
2 Interactive Interface 13
3 System Tray Indicators 13
DESKTOP PROPERTIES 15
1 The Settings Menu: 15
DESKTOP CONFIGURATION OPTIONS 16
1 Shell & Desktop Tab 16
2 Taskbar Tab 20
3 Auto-Start Options Tab 22
TASK MANAGER TOOL 22
4 “How To” Navigate the Task Manager 24

CHAPTER 4 USING THE WBT DIALOG 25

GENERAL TAB 25
1 Advanced 27
2 Make 28
3 System Restore Options: 28
4 Input Tab - Keyboard & Mouse Properties 29
5 Mouse Properties 31
DUAL SCREEN TAB 32
1 Primary Screen 32
2 Monitor settings 32
3 Reposition dialog boxes on 32
4 Connections Settings 32
5 RDP / IE Settings 33
6 ICA configuration for Dual Screen 34
DISPLAY TAB - SETTING THE DISPLAY PROPERTIES 35
1 Display Properties 35
2 Test 35
3 Screen Saver Properties 36
PRINTERS TAB: SETTING CONNECTIONS TO LOCAL/NETWORK PRINTERS 37
1 Defining Local/Network Printers 38
2 Port Settings 39
3 LPT Ports 39
4 COM Ports 39
5 SMB Ports 41
6 LPR Ports 42
7 Print Test Page 43
USB PRINTERS TAB 44
1 Connect a New USB Printer: 44

2 Change USB Printer Properties 45
USB DEVICES TAB 46
1 Power Limit 46
NETWORK TAB - SETTING THE NETWORK CONNECTIONS 50
1 Disable Network Interface (for dialup users): 50
2 Add Network Icon to Taskbar Notification area: 50
3 Prohibit DNS Resolver cache: 51
4 Obtain IP address from DHCP server / Use the following IP address: 51
5 Network Info: 52
6 Manual IP Address: 53
WIRELESS TAB 55
1 Disable Wireless Network Interface: 55
2 Place the wireless adapter at the top of the interface list: 55
3 Add Wireless Icon to Taskbar Notification Area: 56
4 Obtain IP address from DHCP server: 56
5 Use the Following IP address: 57
6 The "Wireless" button: 57
ON/STBY TAB 60
1 Stand-By Mode: 60
2 Log-off: 60
3 Lock Device: 60
4 N/A: 61
5 Device Auto Restart Schedule 61
SECURITY TAB 62
1 Secure Terminal Settings: 62
2 Enable My WBT Setup: 62
3 Publishing Device Access Shortcuts: 62
4 Enable possibility to lock device and add option to start menu: 65
5 Map Logoff to reboot: 66
CERTIFICATE TAB 66
1 Import: Import New Certificate. 67
TIME TAB 67
1 Time Zone 67
2 Session Time 67
SOUND TAB - SETTING THE SOUND PROPERTIES 69
AUTHENTICATION TAB – CONFIGURE THE DEVICE AUTHENTICATION SETTINGS 70
1 Built-in Authentication 70
2 Use Xcalibur Authentication: 70
3 Prompt for smart card info: 70
NETWORK ID TAB 71
1 Enable Access to Network Shares: 71
2 Set Network ID Authentication Behavior: 71
UPGRADE TAB - SETTING SOFTWARE UPGRADE PROPERTIES 73
1 USB Storage: 74
2 Predefined Network Share: 74
3 FTP Server: 75
PLUG-INS TAB 75
1 Downloading a New Plug-in 77
2 Use FTP Server: 78
3 Deleting Plug-in 80
4 Configuring Plug-in Properties 80
LICENSING TAB 81
1 Installed Licenses List 81
2 Installing a New License 82
3 Deleting a License 82

CHAPTER 5 IMAGE 7.0.X – CONNECTIONS MANAGEMENT 84

1 Application Connections: 84
2 Network Connections: 84
3 My Connections 84
4 Connection Mode 85
NEW FEATURES IN MY CONNECTIONS MANAGER 85
PORTAL MODE 88

1 Portal Mode Advantages: 88

CHAPTER 6 NETWORK MANAGER 90

NETWORK MANAGER FEATURES 90
HOW TO USE NETWORK MANAGER 90

CHAPTER 7 XCALIBUR DIALOG – CONFIGURING MANAGEMENT PARAMETERS 92

GENERAL TAB 92
DHCP TAB 94
SERVER LIST 94
1 Servers Operations 95
LOCATOR TAB 97
SNMP TAB 98
PROTOCOL PARAMETERS 98
SOFTWARE DEPLOYMENT 99

CHAPTER 8 RECOVERY AND RESET OPTIONS 102

RESET TO DEFAULT 102
SOFTWARE RESET 102
1 When to use software reset (examples)? 102
HARDWARE RESET & SAFE MODE OPERATION 102
1 What is safe mode? 102
2 Complete the following in order to perform a hardware reset: 102
3 How to do Hardware reset On a Jack PC: 103
4 When to use hardware reset (examples)? 103
REDUNDANT BOOT OPTIONS 103
1 Error Correction 103
2 Disk Surface Check 104
PXE MODE 104
1 What is PXE Mode? 104
2 How Does PXE Recovery Work? 104

CHAPTER 9 IMAGE 7.0.X ADVANCED PLUG-INS CONFIGURATION 106

NEW INTERNET EXPLORER OPTIONS BY CHIP PC 106
NEW FEATURES IN IE 106
HOW TO CUSTOMIZE THE IE PLUG-IN 107
NEW RDP FEATURES INTRODUCED BY CHIP PC 109
1 RDP Seamless Window 110
2 Pass-through Authentication 112
3 RDP Load Balanced Connections 113
4 RDP WAN Optimization 118
5 Minimized RDP Bandwidth 118
6 Disk & RAM Caching 119
7 Bandwidth Compression 119
NEW WINVNC OPTIONS INTRODUCED BY CHIP PC 120
1 Privacy Options 120
KEY CITRIX ICA 11.100 OPTIONS SUPPORTED BY CHIP PC 121
1 Program Neighborhood Agent 121
2 New WinCE PNAgent client options supported by Chip 121

This page is left blank intentionally.

Chapter 1 Preface

The purpose of this manual is to understand Image 7.0.X, familiarize users with the various options of the Windows Desktop Interface, and provide them with the knowledge of how to configure different device's settings and connections locally.

Intended Audience

This manual is aimed at Administrators and end users who want/need to perform management tasks on Chip PC Thin-Client devices without a centralized management system (Xcalibur Global).

Scope

Image 7.0.X for Chip PC Thin-Clients

Objectives

After reading this manual you should be able to:

- Understand Chip PC technology advantages embedded into this image
- Manage access to selected WBT Setup areas
- Implement authentication scenarios
- Configure and customize the Desktop environment
- Take advantage of the 'My Connections Manager' features
- Implement advanced RDP and ICA options
- Use recovery options

Prerequisites

N/A

Reference Materials

N/A

This page is left blank intentionally.

Chapter 2 Introduction to Image 7.0.X

General

Chip PC firmware version 7.0.x image brings a whole new standard to the thin client world, including a wide range of new possibilities integrated into Chip PC thin clients.

A Chip PC firmware image is built of two main layers:

Windows CE Kernel:

Chip PC is using the OS kernel of Microsoft and developed all other components (desktop, plug-ins) in house.

Plug-ins:

Modular software add-ons which can be added and removed from the device according to customer needs.

Plug-ins

Plug-ins are software components that can be integrated into your Thin Client device in order to enable extra functions.

In order to address specific customer needs, Chip PC offers the integration of customized in-house and third party software Plug-ins to Chip PC thin clients.

The Plug-ins are either preinstalled on device or added on the run, according to customer changing needs.

1 Advantages to Using Plug-ins

1.1 Security:

Each plug-in is signed with a digital signature making it impossible to run unsigned software on the device, resulting in full Virus immunity.

1.2 Stability:

Using the plug-in module Chip PC does not change the kernel when installing a new plug-in making it safe to update the operating system.

1.3 Bandwidth:

When changing a specific function in the OS (new ICA version) administrator does not need to send an entire OS image which might be extremely demanding on the organization's network.

Image 7.0 Boot Sequence

The following events should happen during Image 7.0 boot sequence

- Power on
- Bus and peripheral initialization
- Check the stand-by / safe mode button state and entering into following possible state :
  - Reset registry and loading system in Safe Mode: minimal configuration, no plug-in, no Explorer /Shell, no advanced driver
  - Enter into Manual Recovering Mode: search for nearest Xcalibur server and wait for Image Recovery command
  - Load the system in ordinary mode
- Initiate the OS
- Check available storage for disk / flash error
- Check “copy protection”
- Activate available licenses
- Activate network stack : wait for valid IP address (DHCP / Static)
- Activate Xcalibur connection (if needed : local setting / DHCP/policy)
- Waite for connection established
- Waite for Device Policy /Empty Policy
- Activate available plug-ins
- Enter into user mode (local/ remote /auto-logon) (notify Xcalibur)
- Notify Xcalibur about connected user
- Waite for user policies (notify Xcalibur)
- Apply user policy (notify Xcalibur)
- Enter into desktop mode (notify Xcalibur)
- Search / run auto-started connection (notify Xcalibur)

Chapter 3 Desktop Interface Features

Objectives

This chapter, " Desktop Interface Features" introduces the Desktop environment supported by Chip PC thin clients.

The chapter discusses the technical and user-experience differences between the Desktop, PC-Like environment mode and the Legacy Connection Manager mode used previously, as well as going through each feature of the desktop interface with an in-depth explanation and a 'How To' step by step guide.

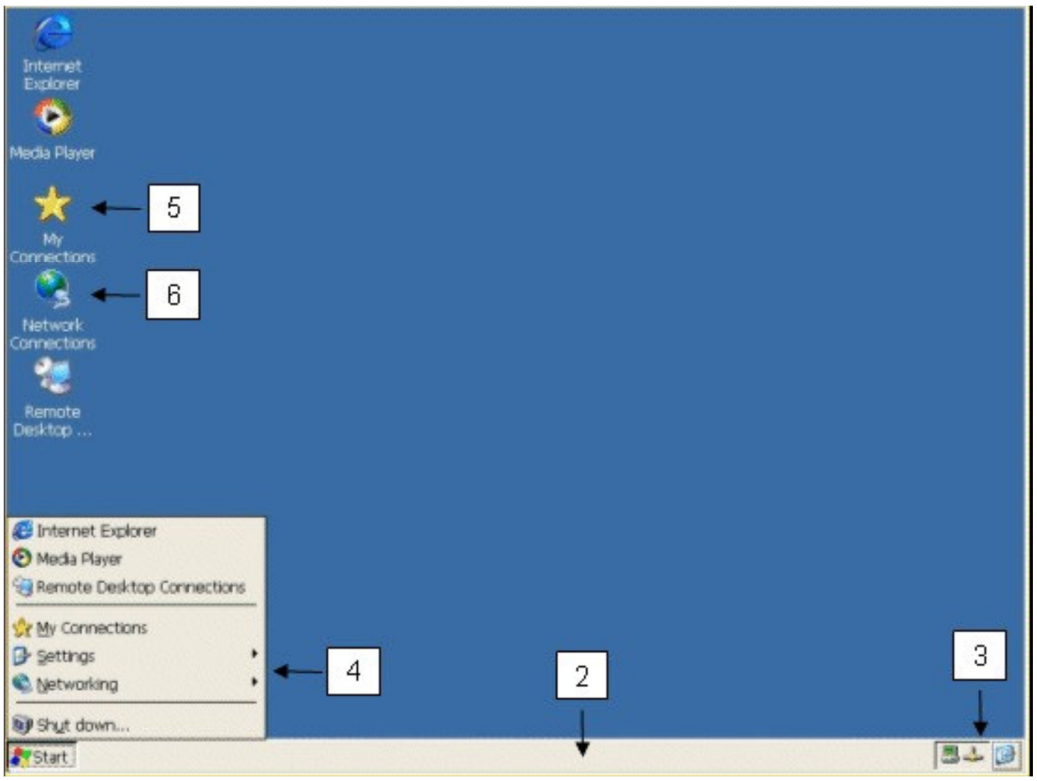
General

Chip PC has released a Desktop interface supported by firmware version 7.0.X. Devices running this firmware display a PC-Like Windows desktop interface.

The desktop interface was designed to answer both friendliness and management needs by being fully customizable. Administrators can easily tailor its looks to fit all their demands combining a PC-Like look & fill environment, with the highest security and manageability offered by Chip PC thin clients.

Desktop Interface Features

The following key features make the desktop interface a perfect solution for those seeking the combination of a Windows Desktop feel & look environment applied on a thin client device.



- (1) True PC-Like Windows interface and behavior
- (2) Real Windows Taskbar area
- (3) Dynamic System Tray area
- (4) Fully customizable Start Menu
- (5) New My Connections Manager tool for session management includes
- various advanced features such as the 'Secured Portal Viewer'.
- (6) New Network Connections tool for network connection management.
- Changeable connection-icons
- Built-in desktop shortcuts support
- Built-in toggling windows support
- Built-in resizable windows support
- Auto-start multiple connections at once
- Changeable Desktop Background Picture

Desktop Interface Advantages

1 User Friendliness and Familiarity

The Start Menu, Taskbar and System Tray interfaces, are all part of the Desktop GUI which now looks closer to an MS Windows Desktop than ever, thus providing users with a 'PC-Like' feel & view similar to that of a Windows Desktop and allowing for a seamless transfer to a TC environment.

2 Interactive Interface

In contrary to the previously used 'Legacy Connection Manager' where users were unaware of the device status, e.g. whether it is connected to the network? Is the externally connected storage actually recognized? Is the IP Printer mapped correctly? What is the device's local time? And so on.

The Desktop interface is interactive and friendly using various System Tray indications notifying users about device status.

3 System Tray Indicators

The System Tray is a dynamic notification area displayed only when working in Windows Desktop mode. Icons displayed in the System Tray indicate users about various system events making their 'work experience' more PC-Like and user friendly.

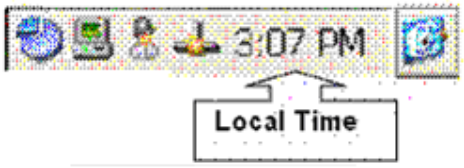
Administrators can control which icons are displayed inside the System Tray area by selecting the Add Icon to Taskbar Notification Area checkbox.

3.1 System Tray Indicator Examples:

- **Network Link Status:** Network Link Status icon in the System Tray provides real-time network indication including TCP/IP properties and network link status (Connected / Disconnected).

- **Storage Manager:** Storage Manager Status icon in the System Tray provides real-time indication for external storage presence, including external storage state, size, file system etc'.

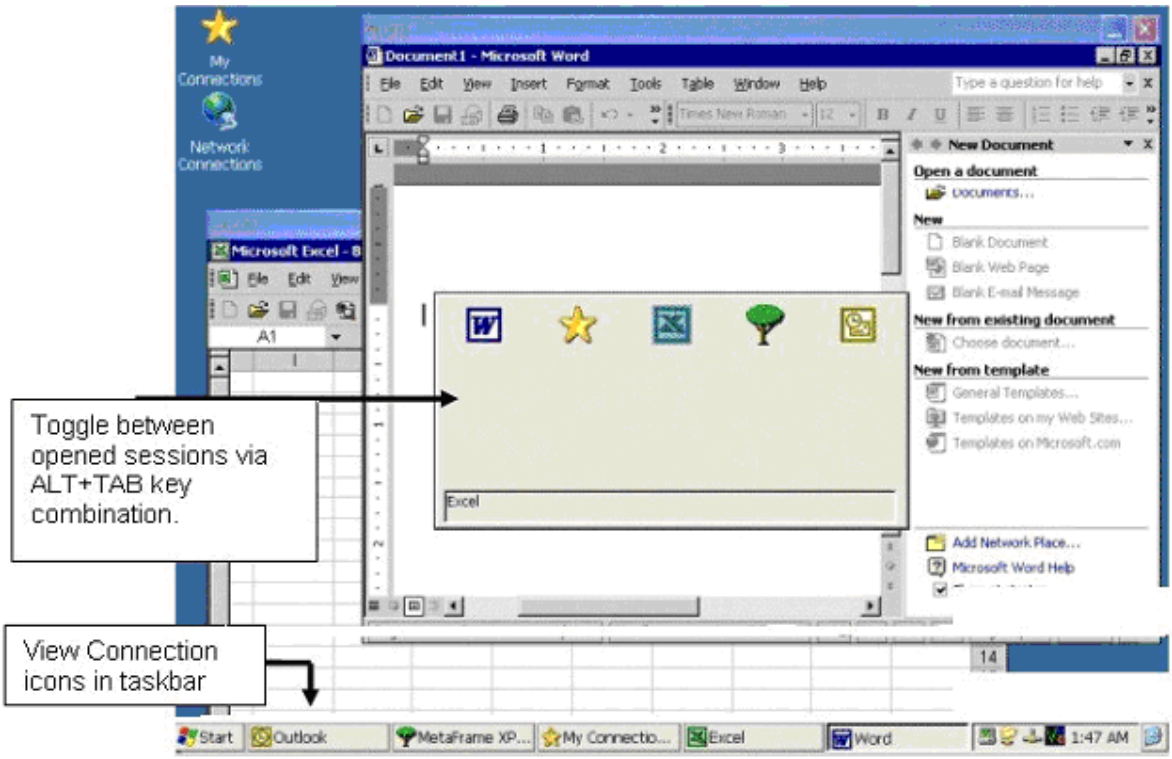
- **Local Time:** Local time Clock icon displayed in the System Tray provides device time properties.



3.2 Easy 'Windows Navigation'

Users will find navigating between Start Menu items, Connections and Taskbar as easy as they are used to, making for an easy transition from PC to TC.

- **Seamless Session Window:** Open 'seamless window' connections and switch between them by ALT+TAB.
- **Desktop Taskbar:** Users can minimize different connection windows onto the Taskbar.
- **Advanced Security:** Avoid Published Desktops via terminal servers to increase security and server performance.



3.3 Fully Customizable

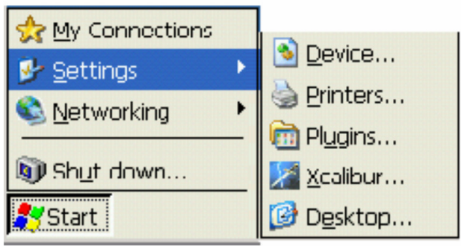
The desktop has a fully customizable interface, ideal for multilevel security environments.

- **Customizable Desktop Icons:** Place Connections icons on the Desktop and change Connections icons to reflect corresponding application.
- **Controllable Start Menu:** All Start Menu items are controllable. Each user's view is a combination of specific menus approved for use of this user by the system manager.
- **Reveal Only Selected WBT Setup Menus:** Allow users to access only necessary WBT Setup menus for their convenient work definitions, while maintaining high security. Decide which menus should be revealed and easily hide all others.

Desktop Properties

1 The Settings Menu:

The Settings menu is the doorway to various device menus, in the Start Settings (GUI menu), there are five submenus:



- **Device:** This shortcut provides access to the full WBT Setup interface which can be considered as the device control panel
- **Printers:** This shortcut provides direct access to the Printers & USB Printers tabs of the WBT dialog.
- **Plug-ins:** This shortcut provides direct access to the Plug-in & Licensing tabs of the WBT dialog.
- **Xcalibur:** This shortcut provide access to different configuration parameters relating to Chip PC Xcalibur Global (see note)
- **Desktop:** This shortcut provides access to the device's desktop configuration parameters

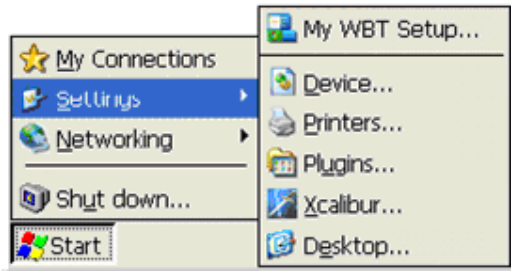
In order to prevent unauthorized users from accessing the default shortcuts you can either password protect the WBT Setup (using the Security Tab) or dim-out any of these shortcuts using the Desktop Interface Taskbar Tab options.

NOTE *Xcalibur Global is Chip PC management software designed for Thin- Client management in large scale environments.*

Desktop Configuration Options

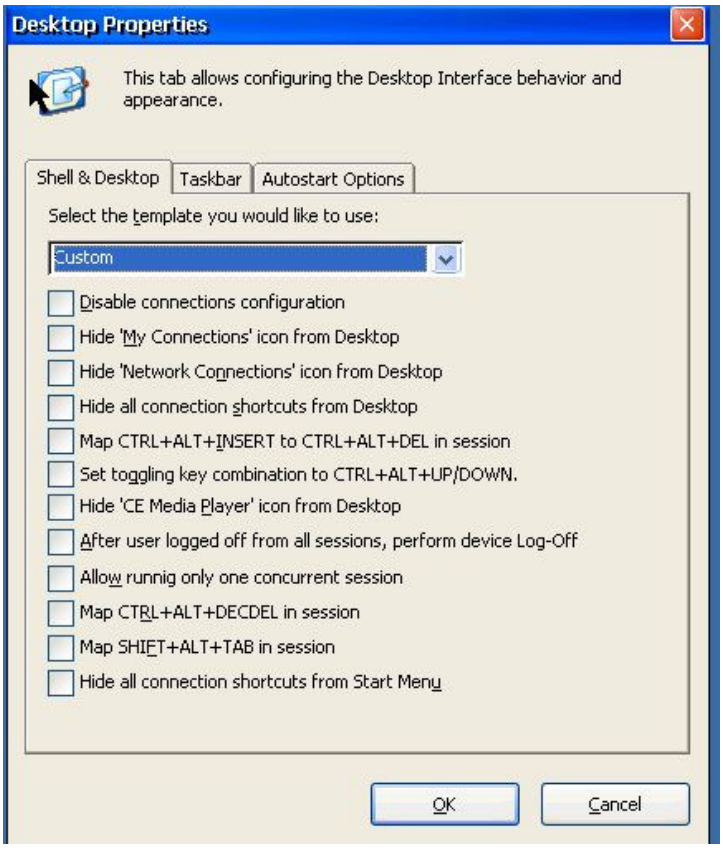
The Desktop Properties Dialog allows for customization of the desktop interface for Chip PC devices. The following describes the customization options which are accessible via the Desktop Properties Dialog.

In order to open the dialog, go to Start → Settings → Desktop



1 Shell & Desktop Tab

Through the Shell & Desktop tab the clients' desktop and connection settings can be customized.


Desktop Properties
This tab allows configuring the Desktop Interface behavior and appearance.
Shell & Desktop
Taskbar
Autostart Options
Select the template you would like to use:
Custom
Disable connections configuration
Hide 'My Connections' icon from Desktop
Hide 'Network Connections' icon from Desktop
Hide all connection shortcuts from Desktop
Map CTRL+ALT+INSERT to CTRL+ALT+DEL in session
Set toggling key combination to CTRL+ALT+UP/DOWN.
Hide 'CE Media Player' icon from Desktop
After user logged off from all sessions, perform device Log-Off
Allow runnig only one concurrent session
Map CTRL+ALT+DECDEL in session
Map SHIFT+ALT+TAB in session
Hide all connection shortcuts from Start Menu
OK
Cancel

1.1 Select the template you would like to use:

Use predefined desktop configurations for ease of management. Scroll down the combo box and selecting one of the following options:

- **None:** Clears all the Desktop options.
- **Custom:** Once changing any of the Desktop Plug-in properties the Template status is automatically set to Custom.
- **Legacy WBT:** Loads predefined Desktop Plug-in options that provide the most simplified working interface. Displaying only the My Connections Manager on the screen.
  The Legacy WBT template selects the following Desktop Properties Dialog settings:

Auto Start Options Tab	Taskbar Tab	Shell & Desktop Tab
Auto Start My Connection Manager	**Always Hide Taskbar**	**Hide My Connections Icon From Desktop**
		Hide Network Connection icon from desktop
		Hide all connection shortcuts from Desktop
		Set toggling key combination to CTRL+ALT+UP/DOWN
		Hide CE-Media player icon from desktop

1.2 Disable connection configuration:

Once marked, modifying or deleting existing connections or creating new ones becomes impossible. Select this option whenever you want to prohibit users from altering connection settings.

1.3 Hide My Connections icon from desktop:

The My Connections manager tool is used to view, modify and delete all the application connections (RDP / ICA…etc) available on a device as well as create new connections.

By hiding the My Connections icon from desktop, only connections which have corresponding desktop shortcuts become available to use. Thus users are limited to only see and use connections that already have desktop shortcuts.

NOTE *The My Connections tool may also be accessible via the Start menu unless set to be hidden from there as described further.*

1.4 Hide Network Connections icon from desktop:

Through the Network Manager tool, users are able to view, modify and delete all the network connections (Dial-up / VPN etc') available on a device as well as create new connections. By hiding the Network Connections icon from desktop, only connections which have corresponding desktop or start menu shortcuts become available for use. Thus users are limited to only see and use connections that have either desktop or start menu shortcuts.

NOTE *Network Manager Tool may also be accessible via the Start menu unless set to be hidden from there as described further).*

1.5 Hide all connection shortcuts from desktop:

Remove all session connections from desktop, denying users the ability to start sessions on their own.

1.6 Map CTR+ALT+INSERT to CTRL+ALT+DEL in session:

Defines the key combination to be used during a session, in oppose to the combination used on the local machine.

1.7 Set toggling key combination to CTRL+ALT+UP/DOWN:

Define the key combination to be used during a session to differ from the combination used to toggle between sessions.

1.8 Hide 'CE Media Player' icon from Desktop:

Remove the media player icon from the desktop disallowing the user the use of media player.

1.9 After user logged off from all sessions, perform device Log-Off:

Once the user logs-off all sessions the machine will perform a reboot.

1.10 Allow running only one concurrent session

Only one remote session will be allowed

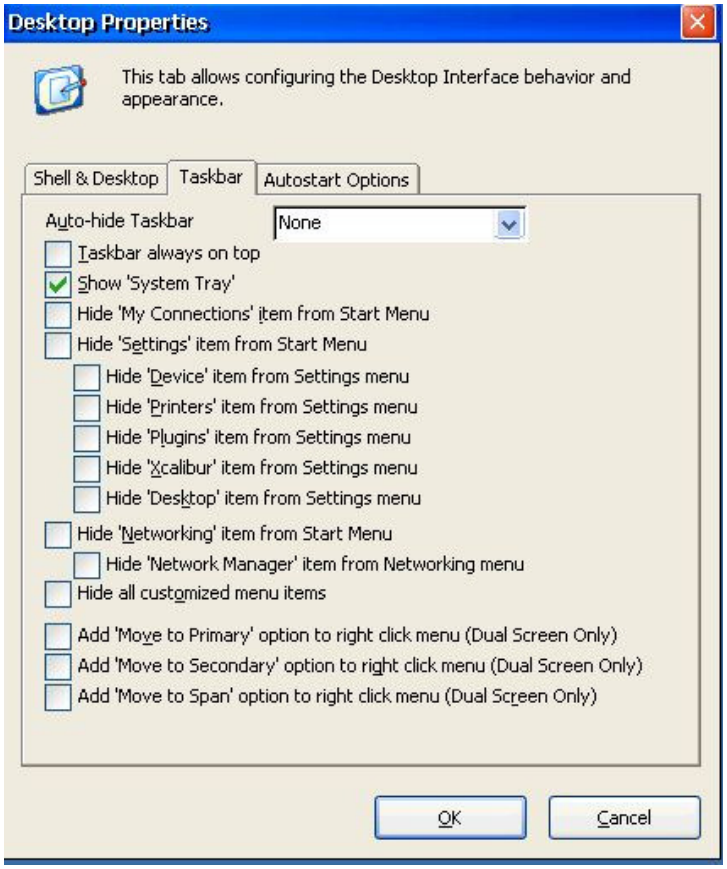
1.11 Map CTRL+ALT+DECDEL in session

1.12 Map SHIFT+ALT+TAB in session

1.13 Map all connectio shortcuts from Start Menu

2 Taskbar Tab

Customize all Start menu and Taskbar items via the Taskbar Tab found under the Desktop Properties Dialog.


Desktop Properties
This tab allows configuring the Desktop Interface behavior and appearance.
Shell & Desktop
Taskbar
Autostart Options
Auto-hide Taskbar
None
Taskbar always on top
Show 'System Tray'
Hide 'My Connections' item from Start Menu
Hide 'Settings' item from Start Menu
Hide 'Device' item from Settings menu
Hide 'Printers' item from Settings menu
Hide 'Plugins' item from Settings menu
Hide 'Xcalibur' item from Settings menu
Hide 'Desktop' item from Settings menu
Hide 'Networking' item from Start Menu
Hide 'Network Manager' item from Networking menu
Hide all customized menu items
Add 'Move to Primary' option to right click menu (Dual Screen Only)
Add 'Move to Secondary' option to right click menu (Dual Screen Only)
Add 'Move to Span' option to right click menu (Dual Screen Only)
OK
Cancel

2.1 Hide Taskbar Options:

Scroll down the combo box and select one of the following options:

- **Auto Hide:** Hides the taskbar.
  To redisplay the taskbar, point to the area where the taskbar is located. To make sure the taskbar is always visible when pointing to it, select the **Taskbar always on top** option.
- **Always Hide:** Permanently hides the taskbar.
  In this mode, in order to logoff or reboot the device, open the My Connections Manager → File menu and select the Exit option.
- **None:** This option will display the Taskbar as default.

2.2 Taskbar always on top:

Ensures that the taskbar is always visible, even when running a program in a maximized (full-screen) window.

2.3 Show System Tray:

Enable the System Tray area.

In order to view notification items in the System Tray select the Show System Tray option. In addition mark the Add Icon to Taskbar Notification Area checkbox (found under various WBT Setup tabs) to view those in the System Tray.

2.4 Hide My Connections icon from Start Menu:

Hide the My Connections item from the Start menu.
Denying users the ability to view the connections defined for the client.

NOTE *My Connections tool may also be accessible via the Desktop menu unless set to be hidden from there as previously described.*

2.5 Hide Settings item from Start Menu:

This option hides the Settings item from the Start menu. The Settings item is an entry point to ALL device menus. Hiding this item prevents local access to any device configuration menus! One must take under consideration that once this option is enabled, device settings become changeable only remotely.

- **Hide 'Device' item from Settings menu:** Dims-out the 'Device…' access shortcut and prevents access to the full WBT Setup environment.
- **Hide 'Printers' item from Settings menu:** Dims-out the 'Printers…' access shortcut. Prevents direct access to the Printers & USB Printers Tabs.
- **Hide 'Plug-ins' item from Settings menu:** Dims-out the 'Plug-ins…' access shortcut. Prevents direct access to the Plug-ins & Licensing Tabs.

2.6 Hide 'Networking' item from Start Menu:

The Network Manager Tool and shortcuts to network connections reside within the Networking item.

- **Hide Network Manage' item from Networking menu:** Hides the Network Manager item from within the Networking menu.

NOTE *'Network Manager' tool may also be accessible via the Desktop menu unless set to be hidden from there as previously described.*

2.7 Hide all customized menu items:

This option hides the 'Start' menu application list and all access shortcuts at once. This option overrides all shortcut options allowing administrators to simplify the ‘Start' menu appearance in a single click.

NOTE *Hiding the Settings item and/or dimming-out the Device… shortcut may prevent access to all local device configuration menus! Therefore making the device highly secured thus device settings become changeable only remotely.*

2.8 Add ‘Move to Primary’ option to right click menu (Dual Screen only)

Adds option to the right click menu. The option is available in devices that upport dual; screen connection

2.9 Add ‘Move to Secondary’ option to right click menu (Dual Screen Only)

Same as previous option

2.10 Add ‘Move to Span’ option to right click menu (Dual Screen only)

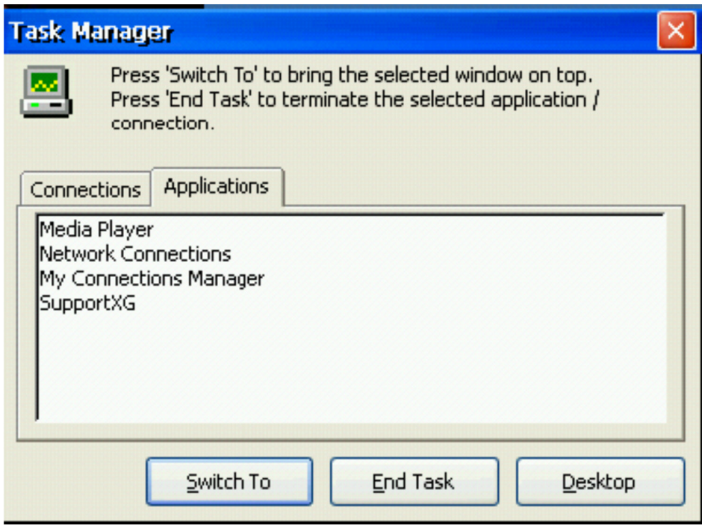
Same as previous option

3 Auto-Start Options Tab

The Auto-start Options Tab specifies whether the My Connections Manager and/or the Network Manager tools will be opened automatically at the end of the device boot.

Task Manager Tool

The Task Manager tool displays details about active connections and applications running on the device. In addition, it provides indications about device performance and allows users to switch between open applications and to end programs.


Task Manager
Press 'Switch To' to bring the selected window on top.
Press 'End Task' to terminate the selected application / connection.
Connections
Applications
Media Player
Network Connections
My Connections Manager
SupportXG
Switch To
End Task
Desktop

4 "How To" Navigate the Task Manager

4.1 Open Task Manager:

The Task Manager can be accessed in two ways.

- Press the CTRL+ALT+DEL key combination (Using the Shell & Desktop tab of the Desktop properties tool it is possible to map the above key combination to CTRL+ALT+Insert)
- Double Click the Task Manager System tray icon.

4.2 Switch between running connections / applications:

Select a connection name from the Connections Tab or an application name from the Application Tab and press the Switch To button.

4.3 Stop a running connection / application:

Select a connection name from the Connections Tab or an application name from the Application Tab and pressing the End Task button.

4.4 Minimizing all windows to desktop:

Press the Desktop button.

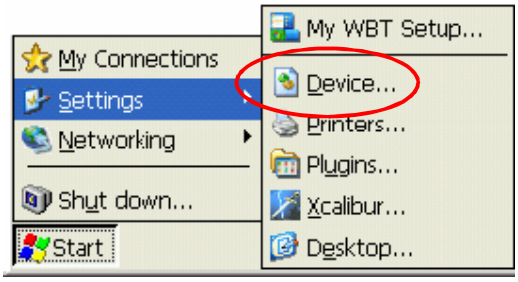
4.5 View device load indication:

Device load factor is hardware model dependent. General device strength is often measured by the number of simultaneous sessions it can carry. The Task Manager tool provides a graphical indication of device loads by changing the system tray icon color incase of resource loss. The default Task Manager System Tray icon color is green. Incase of device resource loss the Task Manager System tray icon color turns red indicating low system resources. To free resources, close any unused applications / connections.

Chapter 4 Using the WBT Dialog

This section explains the various options of the WBT Setup interface, which can be seen as the control panel for the Thin Client device.

To change any of the device settings locally open the WBT Dialog by clicking on Start → Settings → Device.



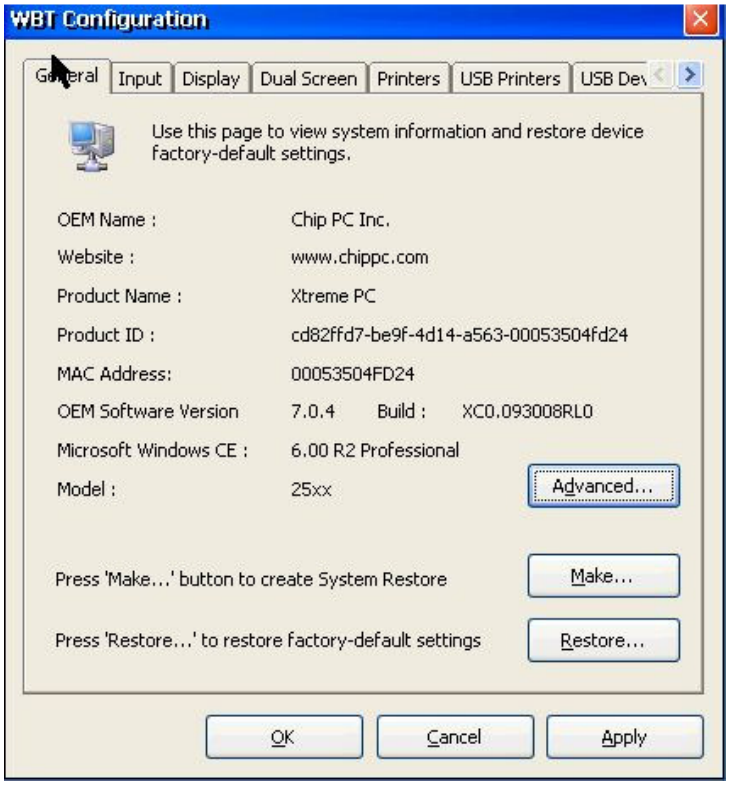
The WBT dialog box consists of various tabs each controls a different aspect of the device's configuration.

The following properties Tabs are used to control device properties:

NOTE *Variation in hardware may result in slight variation is the WBT Dialogs some tabs may appear only with supporting hardware.*

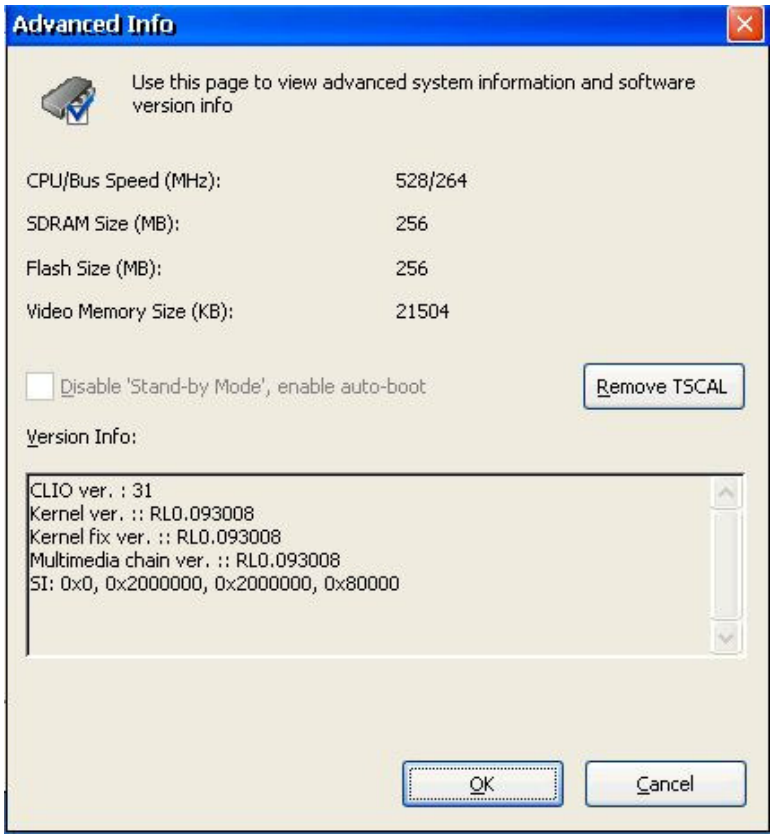
General Tab

This interface provides general device information such as product ID, MAC address OEM software version etc'. Using this tab you will also be able to Create System restore and Reset to device to factory defaults.


WBT Configuration
General
Input
Display
Dual Screen
Printers
USB Printers
USB Dev
Use this page to view system information and restore device factory-default settings.
OEM Name :
Chip PC Inc.
Website :
www.chippc.com
Product Name :
Xtreme PC
Product ID :
cd82ffd7-be9f-4d14-a563-00053504fd24
MAC Address:
00053504FD24
OEM Software Version
7.0.4
Build :
XC0.093008RL0
Microsoft Windows CE :
6.00 R2 Professional
Model :
25xx
Advanced...
Press 'Make...' button to create System Restore
Make...
Press 'Restore...' to restore factory-default settings
Restore...
OK
Cancel
Apply

1 Advanced

Click on the 'Advanced' button to view in-depth hardware details.


Advanced Info
Use this page to view advanced system information and software version info
CPU/Bus Speed (MHz): 528/264
SDRAM Size (MB): 256
Flash Size (MB): 256
Video Memory Size (KB): 21504
Disable 'Stand-by Mode', enable auto-boot
Remove TSCAL
Version Info:
CLIO ver. : 31
Kernel ver. :: RL0.093008
Kernel fix ver. :: RL0.093008
Multimedia chain ver. :: RL0.093008
SI: 0x0, 0x2000000, 0x2000000, 0x80000
OK
Cancel

- **Remove TSCAL:** Remove licenses from the client. This option will remove the license from the client while leaving all other settings in place.
- **Viewable hardware parameters:**
  - CPU/Bus Speed (MHz)
  - SDRAM Size (MB)
  - Flash Size (MB)
  - Video Memory-Chip Size (KB)

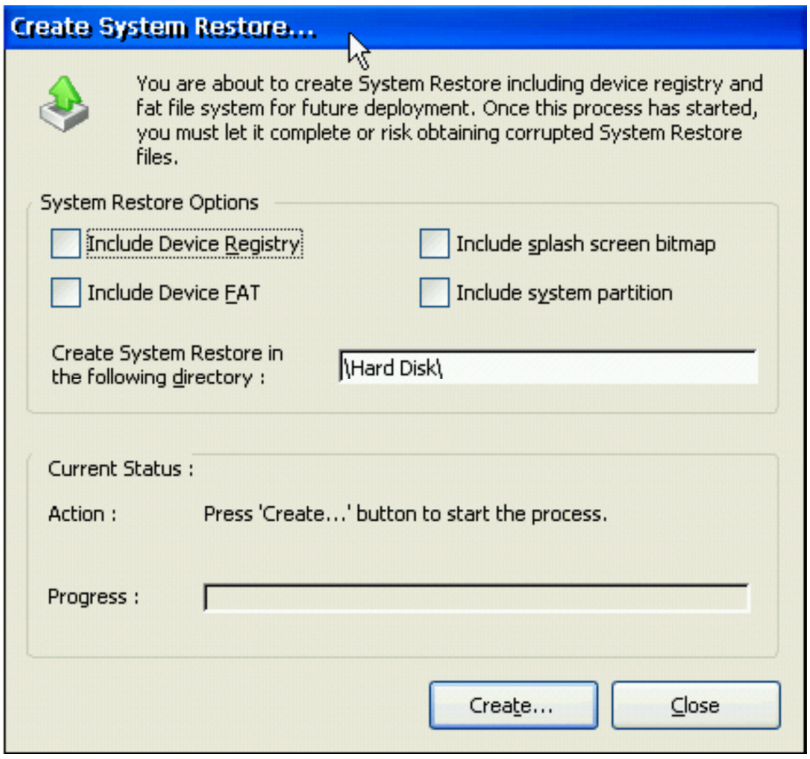
2 Make

The Make option enables users to create a full or partial system restore image that can be used as backup or to configure other units.

Users can define which parts of the image to save and the location of the saved image.

Unique information (such as: MAC address, CPU number etc.) is saved dynamically making it possible to load a system restore image from one device to another

Using System Restore is also supported through the Upgrade tab of the WBT dialog enabling users to upgrade their device using a system restore image.


Create System Restore...
You are about to create System Restore including device registry and fat file system for future deployment. Once this process has started, you must let it complete or risk obtaining corrupted System Restore files.
System Restore Options
Include Device Registry
Include splash screen bitmap
Include Device FAT
Include system partition
Create System Restore in the following directory :
\Hard Disk\
Current Status :
Action :
Press 'Create...' button to start the process.
Progress :
Create...
Close

3 System Restore Options:

- Include Device Registry
- Include Device FAT
- Include splash screen bitmap
- Include System Partition

NOTE *Always select all checkboxes in order to create a full system restore image. Leaving one or more checkbox unmarked means that a partial image will be created. Partial image should only be made under directions from a member of Chip PC staff.*

3.1 System Restore target directory:

Users can define the target location of the system restore image. The default path: \Hard Disk\ is used to save the image on a DiskOnKey. If you want to use a shared location define it as below:
\\computer name\shared folder

NOTE *Creating a System Restore removes all licenses installed on the device. Make sure all license for the source device are either saved in the Xcalibur Global DB or locally.*

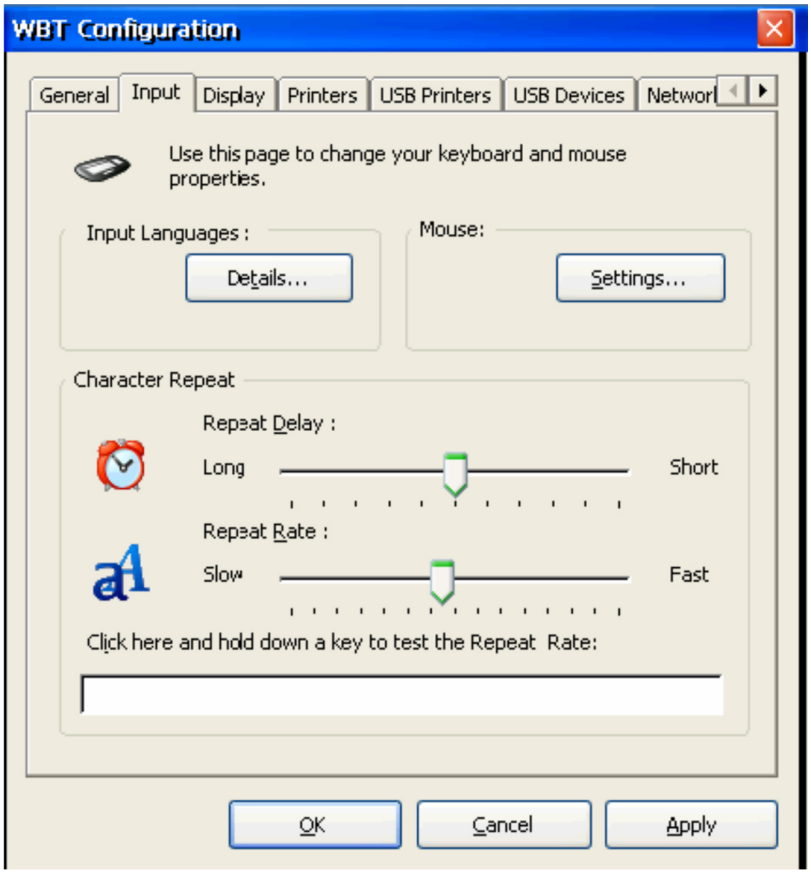
NOTE *Using a shared location or a USB flash storage device is only possible after enabling these options under the Network ID and USB devices tabs.*

3.2 Reset

For a complete explanation on Reset options (including Reset to Factory Defaults under General tab) refer to Chapter 8 of this document.

4 Input Tab - Keyboard & Mouse Properties

Set keyboard settings including language, and mouse properties.



4.1 Input Languages

Chip PC image 7.0.X has a built in support for German and French system dialogs, this means that application icons can appear in those languages by changing the default input local to either language.

It is also possible to switch between different input local using different key combinations.

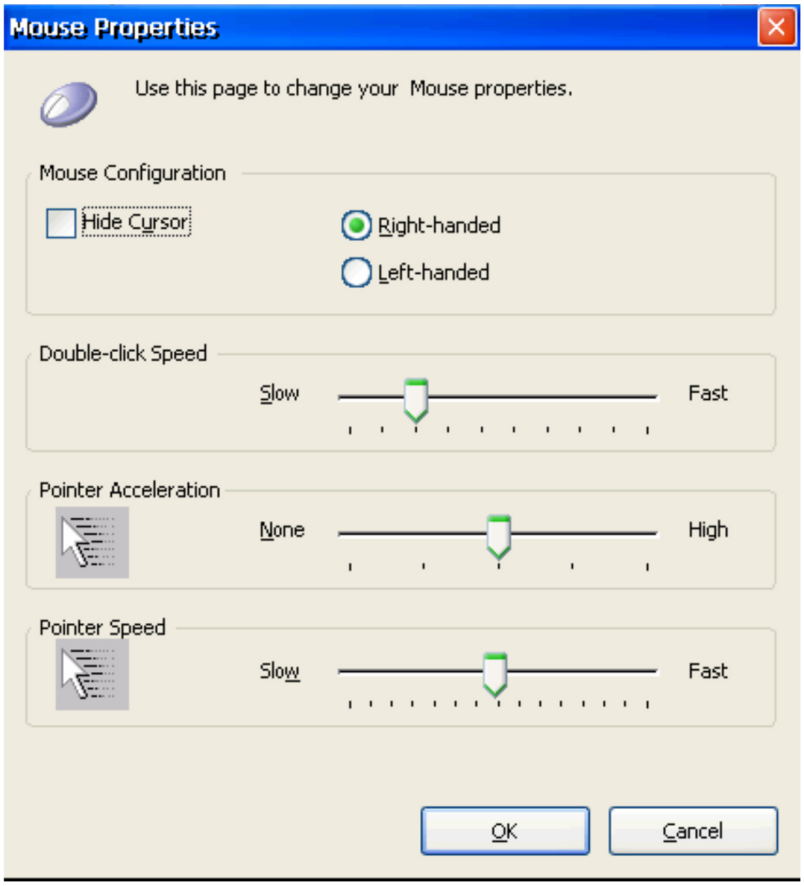
To change default language:

- Click the Details button to open the input language window.
- In the Select default input language, choose English, German or French.
- In the Select installed input Languages to use select the input languages to be used by marking the appropriate checkboxes.
- In the Hot Keys for input locals Dropdown menu choose which combination will be used to switch between input locals.
- The Enable indicator on Task Bar will add an icon to the task bar. Mark the checkbox to add an icon indicating with language is currently in use.
- NumLock on Boot mark this checkbox for the keyboard to activate NumLock automatically following a system boot.
- Reboot Client in order for changes to take effect.

NOTE *Changing the default input language to any other language will not change the image itself (which means that the application icons and system dialogs will remain in English).*

5 Mouse Properties

Under the Mouse section of the Input tab click on Settings, the Mouse Properties dialog will appear.



- Hide Curser: Mark to replace the mouse curser with a dot in order to make it invisible to users.
- Choose the Radio Button Left handed or Right handed to choose which button you will use on your mouse for double-clicking. The default is Righthanded.
- Double Click Speed: Define the rate of your mouse double click.
  Pointer Acceleration Slider: Use to adjust the acceleration rate of the mouse.
- Pointer Speed Slider: Use to adjust the speed of the mouse cursor movement on the screen.
- Click OK to returns to the Input tab and saves changes.
- Click Cancel to returns to the Input tab, without saving the changes.

5.1 Keyboard Properties

The Character Repeat frame is used to set the keyboard character repeat parameters:

- **Repeat Delay Slider:** Adjusts the repeat delay of keyboard characters. The Repeat Delay slider determines how quickly the same character will appear on screen when typed more than once.
- **Repeat Rate Slider:** Adjusts the repeat rate of a keyboard character. Repeat Rate determines how quickly the same character will appear on screen when the associated key is held down.

Dual Screen tab

The Dual Screen tab enables users to configure different Dual Screen related parameters on Chip PC devices.
Additional configuration is done on a per connection bases.

NOTE *Only devices that support dual screen functionality (EFI-6900, EX- 65XX, 66XX) will have this tab.*

1 Primary Screen

The primary screen is the screen that by default all system dialog including task bar and log-in screen will be opened on. The primary screen should be positioned on the left in order to ensure smooth mouse operation.

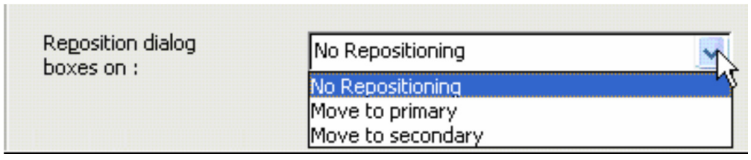
2 Monitor settings

Use this option to configure image appearance on the devices monitors.

- **DVI Monitor:** DVI monitor connected only
- **Clone mode:** Both screen show the same image

3 Reposition dialog boxes on

Use this drop down menu to reposition system dialog boxes when using horizontal span. By default system's dialog boxes will be opened in the center of the "wide screen" meaning the first half will be in the primary screen and the second half will be in the secondary screen.



- **Move to primary:** All system dialog boxes will be opened on the primary screen.
- **Move to secondary:** All system dialog boxes will be moved to the secondary screen.

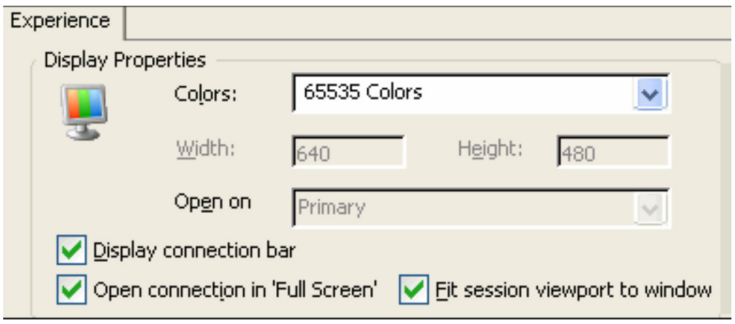
4 Connections Settings

In order to enable the use of Dual screen mode certain settings needed to be configure on each connection or plug-in.

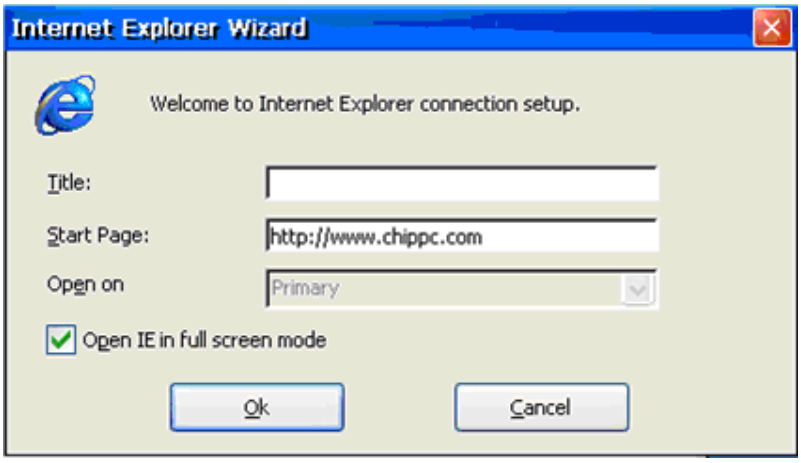
5 RDP / IE Settings

When a new RDP / IE Connection is created, users can define where to open this connection (primary, secondary) through the Open on drop down menu.

- RDP



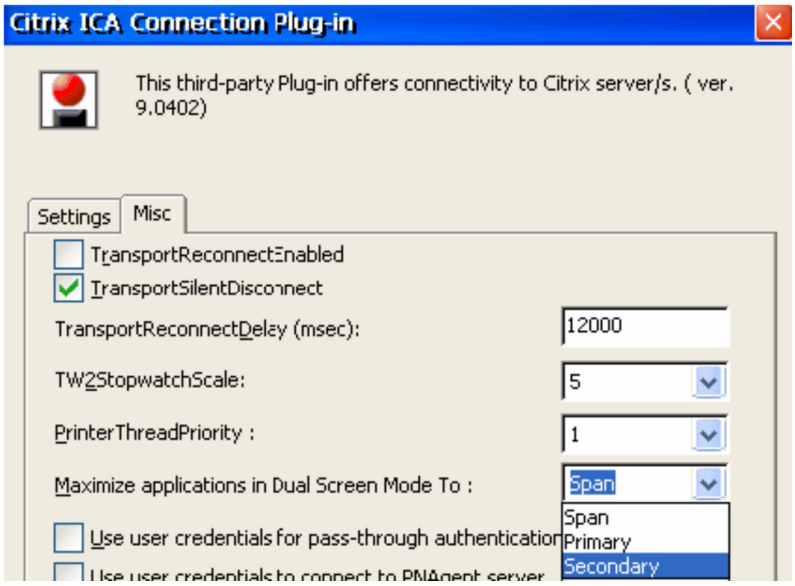
- IE



6 ICA configuration for Dual Screen

Under the Plug-ins tab, select the Citrix ICA Connection, and click on the Configure button.

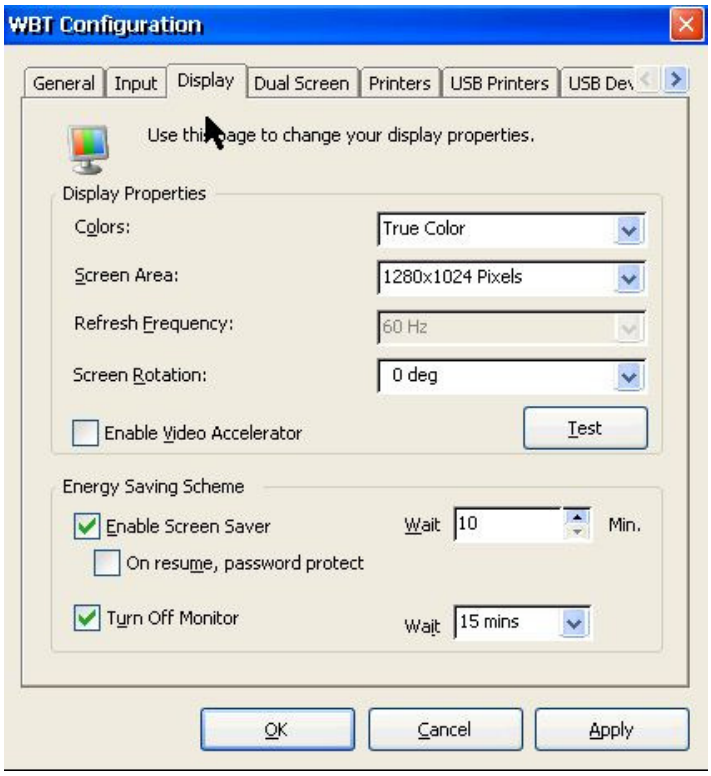
Under the Misc tab go to the option "Maximize application in Dual Screen Mode To:" (as shown below).



NOTE *Dual screen is supported only in ICA plug-in version 9.0402 or later.*

Display Tab - Setting the Display Properties

The Display tab is used to set display and screen saver properties.



1 Display Properties

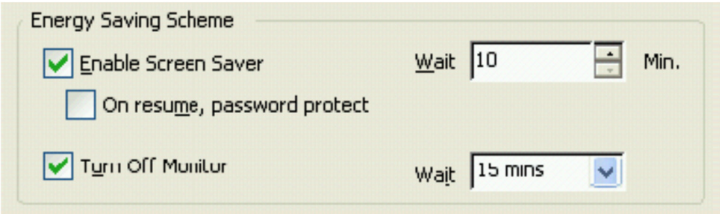
- **Colors:** Choose the colors resolution you wish to set for your display. The default is 256 colors.
- **Screen Area:** Choose desktop resolution. The default is 640x480 pixels.
- **Refresh Frequency:** Choose refresh frequency fit for your screen.
  The default is 60 Hz.
- **Screen Rotation:** Select the rotation angle of the screen. The default is 0 deg
- **Enable Video Accelerator:**

2 Test

Provides a preview of the settings chosen, and allows user to retreat to previous settings if needed.

- Click on the Test button to begin testing, a Testing Mode message will appear.
- Click OK to accept and start testing mode.
- Click either on Yes or NO to accept or reject changes to the display settings.

3 Screen Saver Properties

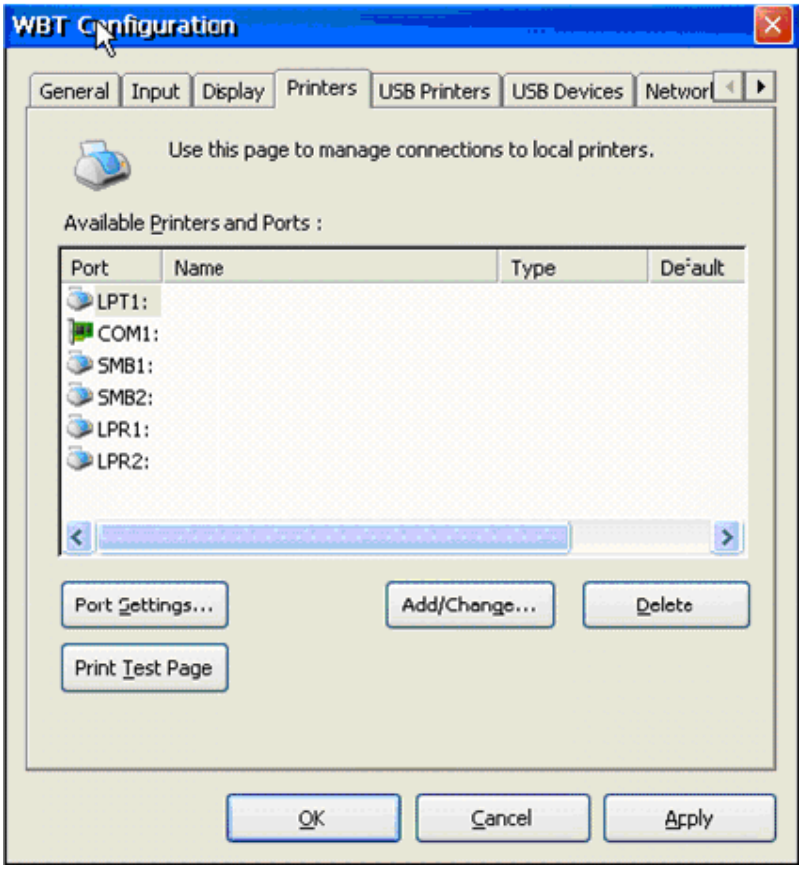


- **Enable Screen Saver:** Mark the checkbox to activate the screen saver. By default it is activated. The Wait option adjusts the amount of time (in minutes) that elapses before the energy saver starts. By default the amount of time for activating the screen saver is set to 5 minutes.
- **On resume, password protect:** Mark the checkbox to prompt the user for credentials as he resumes work with the device. This option is only functional when used in Domain Authentication mode applicable through Xcalibur Global.
- **Turn off Monitor:** Mark this checkbox to activate the power-saving feature of turning off the monitor when the mouse and keyboard are not activated for a specified period of time. By default it is activated. The Wait option adjusts the amount of time (in minutes) that elapses before the turn off monitor starts. By default the amount of time for turning off the screen is set to 10 minutes after the mouse and keyboard are not activated.

Printers tab: Setting Connections to local/network Printers

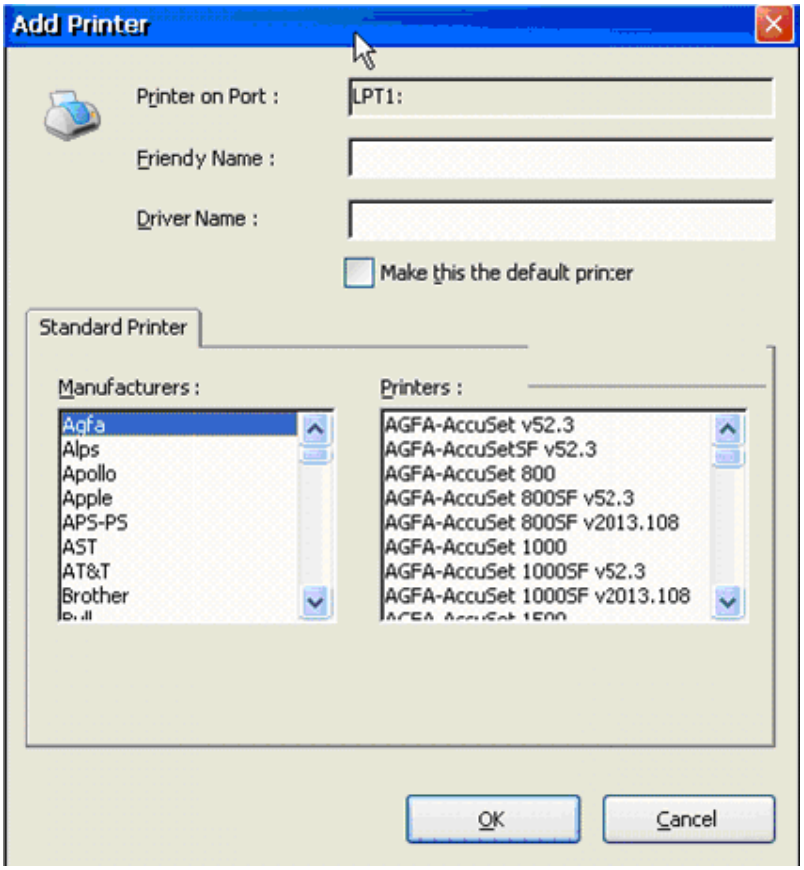
The Printers Tab provides an interface from which locally/network attached printers are configured and managed.

NOTE *In order to map any printer to a session both connection and server side settings are required.*



1 Defining Local/Network Printers

- Press Add/Change and Delete buttons to add/edit and delete printers connected to the COM1, LPT1, SMB1, SMB2, LPR1 and LPR2 ports of the device.
- Choose port type to which you wish to connect the local printer to.
- Pressing Add/Change button will open the screen for defining printer properties.



- Printer on Port Displays the port on which the printer is set.
- Friendly Name Choose\ Edit a name for the printer which will be easy for the user to locate on the network.
- Driver Name Provide a name manually for the driver. (this will be done when a printer is a non-standard printer and does not show in the list box)
- Make this the default printer Mark this checkbox to define a printer as default.
- Standard Printer In case the printer is a standard printer, choose it from the Predefined List Boxes according to Manufacturer and Printer Model.
- Click on OK/Cancel to accept the new printer or Cancel to return to previous screen without saving changes.

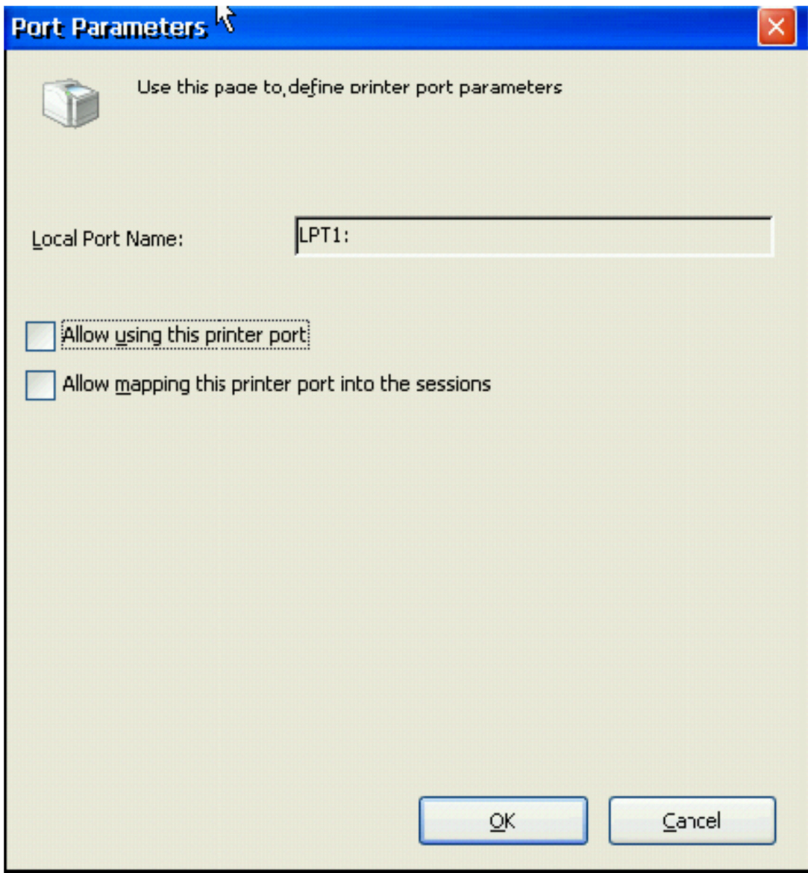
NOTE *For a non-standard printer to be recognized by the Chip PC thin-clients the printer drivers should be installed on the server and the printer manufacturer and model defined.*

2 Port Settings

In order to control the Port Settings:

- Select the port you wish to configure
- Press Port Settings

3 LPT Ports

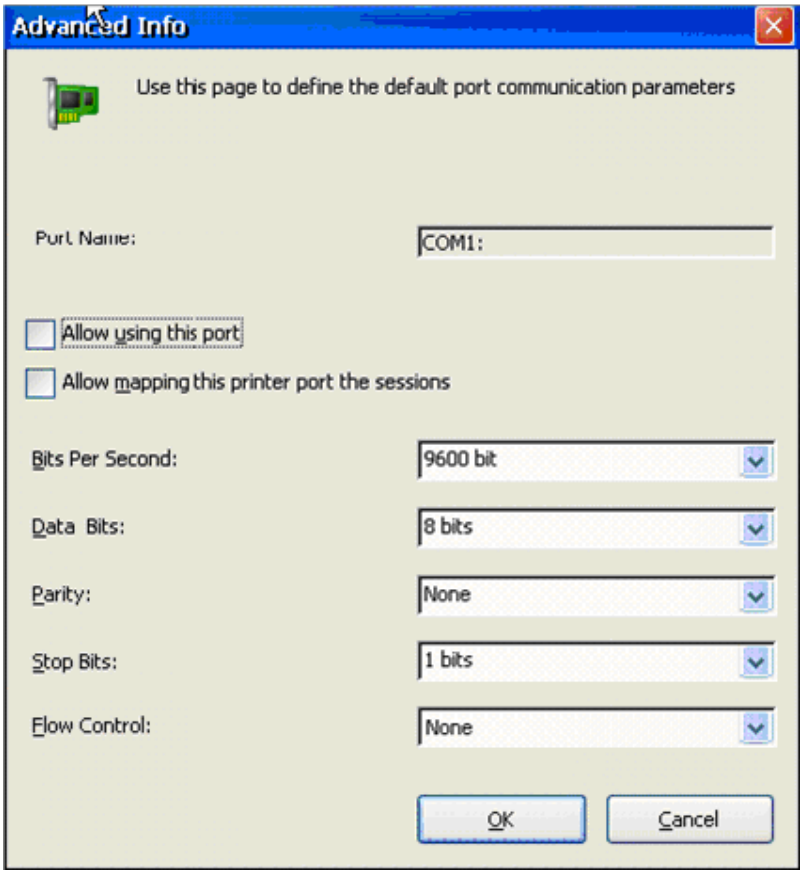


- Allow using this port: By checking this checkbox user allow printers to connect to this port
- Allow mapping this port into the sessions: By checking this checkbox user allow to map printers from this port to a session

4 COM Ports

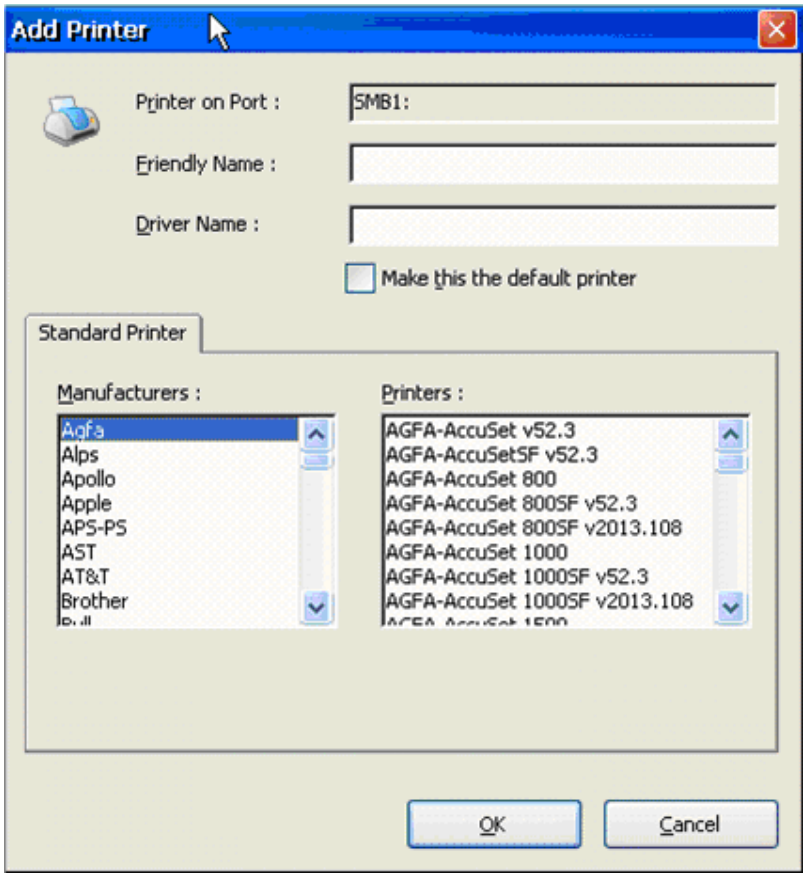
COM ports are often used by serial printers / barcode readers and various other serial devices which can be mapped into a terminal session. Controlling port speeds and bound rates provide improved connectivity with locally attached serial devices which may require unique settings for fluent communication.

For COM port definitions select the port and click on Port Settings.



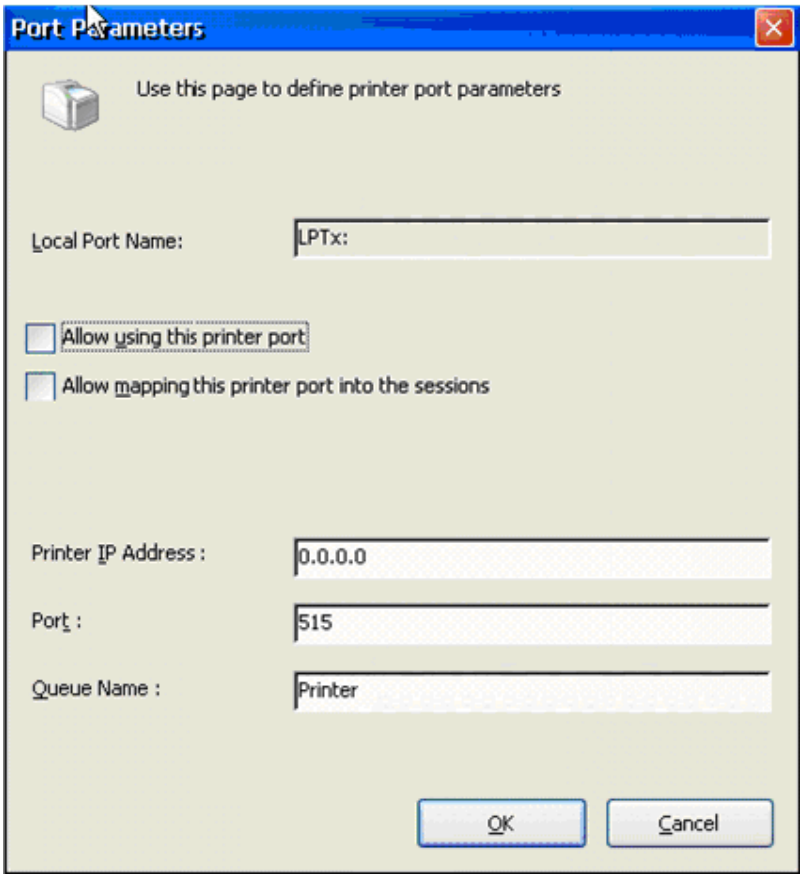
- Allow using this port: Mark this checkbox to allow printer connection to this port
- Allow mapping this port into the sessions: Mark this checkbox to allow users to map printers from this port to a session
- Port Name: Indicates the name of the port in use.
- Allow using this port: Mark checkbox to allow printers to connect to this port.
- Allow mapping this printer port the session: Mark checkbox to allow connection from this port to session.
- Bits per Second: Define the maximal bandwidth allocated for the print job.
- Data Bits: Changes the number of data bits you want to use for each character that is transmitted and received. The computer or device you are communicating with must have the same setting that you choose here. Most characters are transmitted in seven or eight data bits.
- Parity: Define whether to use parity as a mechanism to validate the data transfer
- Stop Bits: Change the time that passes between each character being transmitted (where time is measured in bits per second).
- Flow Control: Changes how the flow of data is controlled. Xon/Xoff, sometimes called software handshaking, is the standard software method of controlling data flow between two modems. Hardware flow control, sometimes called hardware handshaking, is the standard method of controlling data flow between a computer and a serial device.

5 SMB Ports



- Allow using this printer port: Mark checkbox to allow printers to connect to this port
- Allow mapping this port into the sessions: Mark checkbox to allow mapping printers from this port to a session
- Network Printer Share: Enter your computer and printer name (Only computer name not IP address will be accepted).

6 LPR Ports

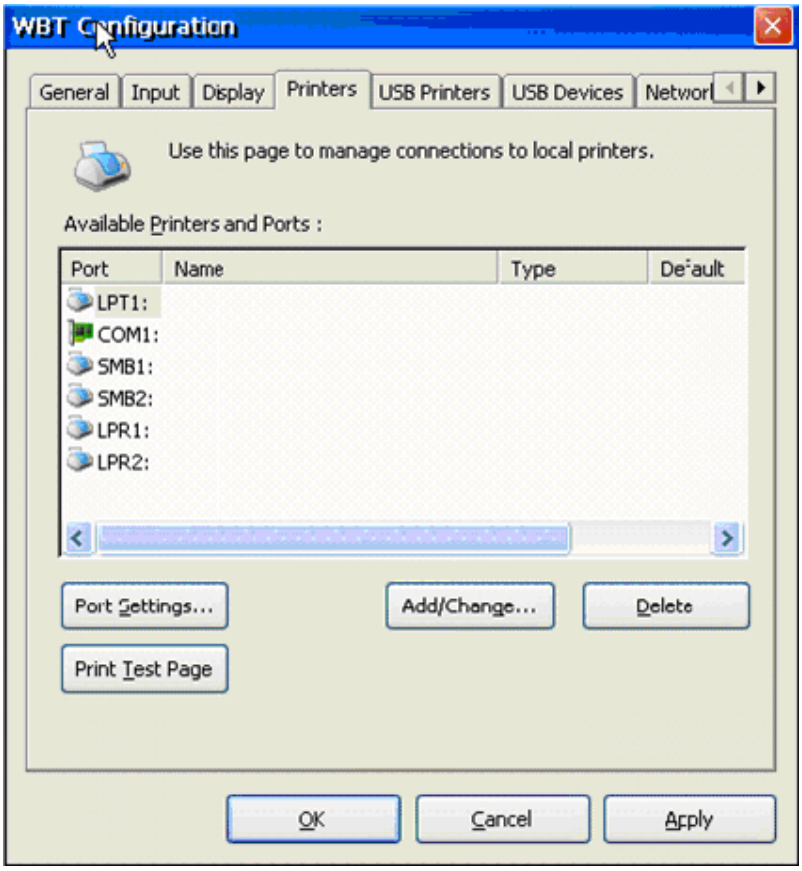


- Local Port Name: Indicates the name of the port in use.
- Allow using this port: By checking this checkbox user allow printers to connect to this port
- Allow mapping this port into the sessions: By checking this checkbox user allow to map printers from this port to a session.
- Printer IP Address: Type the Printers IP address
- Port: Port number in use
- Queue Name: The name of the queue.

7 Print Test Page

In order to verify the accuracy of settings applied on a locally attached printer as well as testing the physical communication between that printer and the device, pressing the Print Test Page button triggers a test page to be printed directly from the device to the printer attached to it. Successful print, suggests device-printer settings are correct.

This feature is ideal for troubleshooting terminal server printer mapping cases, since it immediately indicates whether a printing problem origin is server or client related.

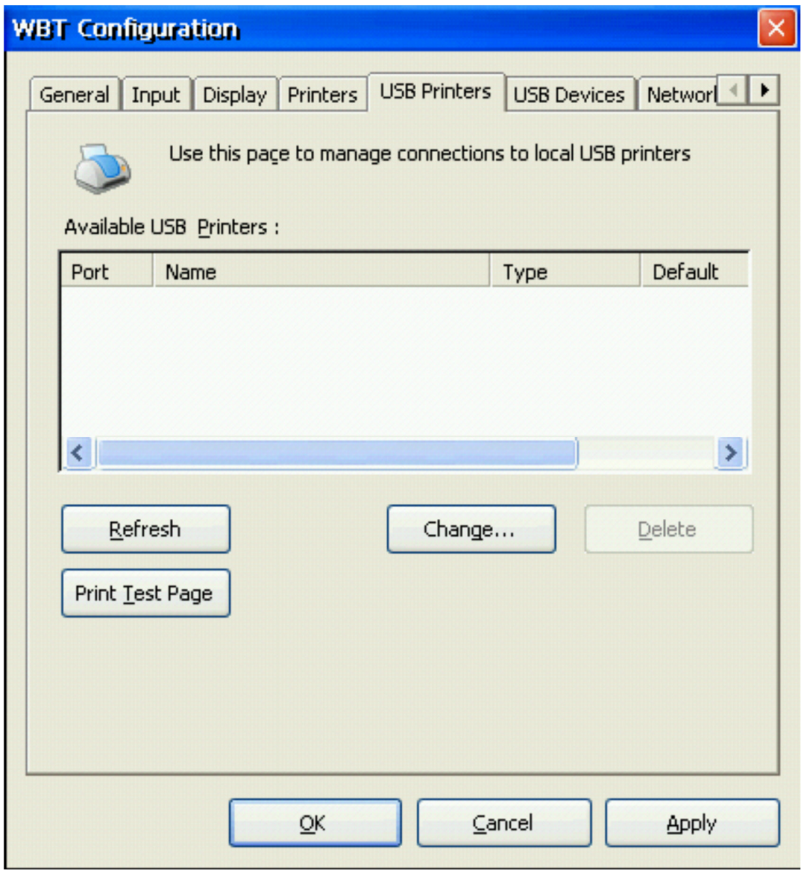


NOTE *The Print Test Page option is also available under USB Printers Tab.*

USB Printers Tab

The USB Printers tab controls the recognition and settings of local USB printers connected directly to the device.

The Available USB Printers list box displays a list of local USB printers, which are connected to the device.

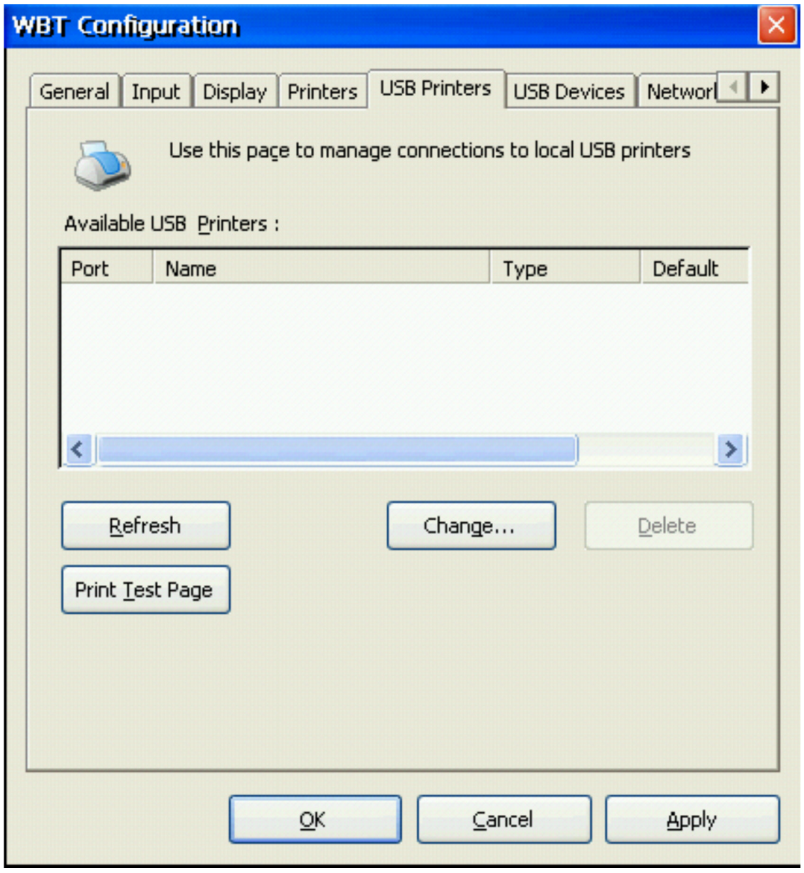


NOTE *The device's USB ports are Plug & Play ports. Therefore the device detects the USB printer automatically when connected to the port.*

1 Connect a New USB Printer:

- Connect the printer to one of the USB ports. Make sure that the printer is "On". It is preferable that the USB printer will be connected to the device prior to turning the device On, In this case the USB printer will be recognized automatically and mapped to session.
- In case the printer is connected once the device is already on, the USB printer will be recognized but the device will have to be restarted to enable mapping of the printer to sessions.
- The printer name will be displayed in the Available USB Printers List. If it is not presented, press the Refresh button.

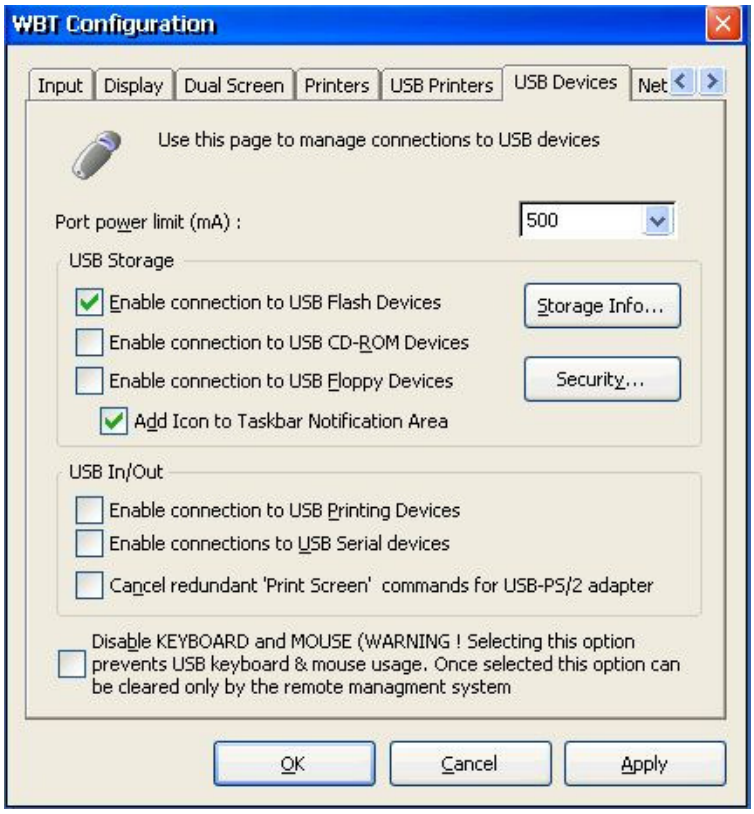
2 Change USB Printer Properties



- Select the printer from the Available USB Printers list and click the Change button. This will open the selected printer's properties window.
- The printers Friendly Name and Driver Name will appear and can be modified.
- The selected USB printer can be also defined as the default printer.

USB Devices Tab

USB Devices tab is dedicated for USB devices management allowing users to define general device behavior regarding USB Storage and other HID devices.


WBT Configuration
Input
Display
Dual Screen
Printers
USB Printers
USB Devices
Net
Use this page to manage connections to USB devices
Port power limit (mA) :
500
USB Storage
Enable connection to USB Flash Devices
Storage Info...
Enable connection to USB CD-ROM Devices
Enable connection to USB Floppy Devices
Security...
Add Icon to Taskbar Notification Area
USB In/Out
Enable connection to USB Printing Devices
Enable connections to USB Serial devices
Cancel redundant 'Print Screen' commands for USB-PS/2 adapter
Disable KEYBOARD and MOUSE (WARNING ! Selecting this option prevents USB keyboard & mouse usage. Once selected this option can be cleared only by the remote managment system
OK
Cancel
Apply

NOTE *The Prohibit connections to USB input Devices checkbox will block all use of USB devices.* ***DO NOT*** *mark this check box since this will prohibit users use of USB keyboard and mouse.*

1 Power Limit

In some cases USB devices connected to the thin client require more power than the default. Use this drop down menu to define the USB port power limit (it is also possible to type the required power).

NOTE *It is not recommended to use more than 750 mA as the power limit.*

1.1 USB Storage

Since connecting local USB storage might become a security hazard, by default all USB storage devices (e.g. USB Floppy / Disk-On-Key / Memory Reader…etc) are not recognized.

By using the checkboxes in this section of the dialog you can enable usage of different USB storage devices.

Add Icon to Taskbar Notification Area:

Mark the checkbox to view a Storage Icon that is dynamically displayed in the System Tray once an external USB Storage device is connected and recognized by the device.

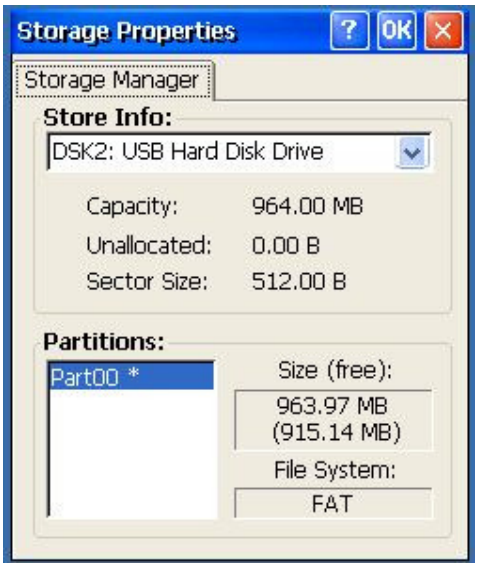
1.2 USB In/Out

Use the check boxes to enable or disable other USB devices.

NOTE *By marking this checkbox you will make all USB input devices including mouse and keyboard unusable.*

1.3 Storage Info

The Storage Manger utility provides general storage details regarding an externally connected USB storage device. Total storage size, file system type and amount of free space information are displayed by pressing the Storage Info button in the USB Devices Tab.



1.4 Connecting a USB storage device

- Connect the USB Storage device to one of the free USB ports.
- The USB storage device is mounted automatically to the local file system.
- It is preferable that the USB device will be connected to the device prior to turning the device on; in this case the USB Storage device will be recognized automatically.
- In case the USB device is connected once the device is already on, the device will have to be restarted to enable recognition of USB device

1.5 Storage Mapping

Storage Mapping enables to map a local storage into ICA or RDP session and mount it as additional drive letter.

To Enable Storage Mapping:

- Enable the appropriate storage device from the USB Storage section of the USB Devices dialog.
- The RDP or ICA protocols at the client side must be configured to support Storage Mapping (for details see below).
- The Citrix or Terminal Servers must be configured to support storage mapping.

1.6 Enable Storage Mapping in RDP Session

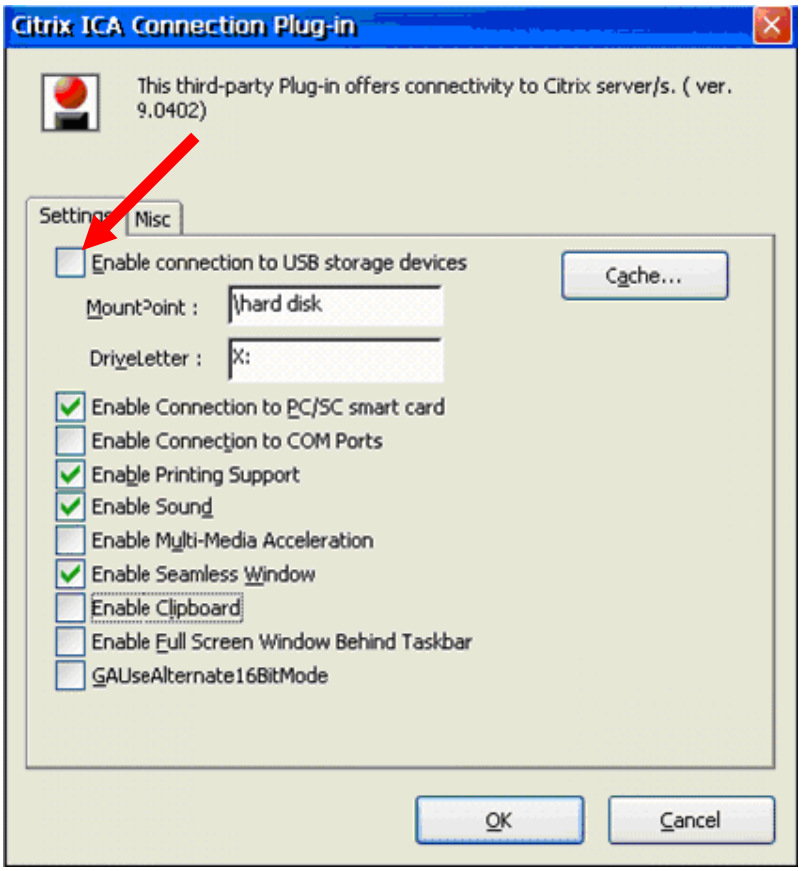
- From the My Connections dialog choose the RDP connection name, right click and press Properties.
- Choose the Local Resources tab from the RDP Connection Setup windows
- Check the Local Storage check box.
- Press OK.
- Enable Storage Mapping in the Windows Terminal Server configuration.

Local devices
Connect automatically to these local devices when logged on to the remote computer:
Printers
Local Storage
Serial ports
Smart Card
Don't warn me before connecting local device(s) to server

NOTE *RDP Storage mapping functionality is supported only in Windows 2003 Terminal Server; it is not supported in Windows 2000 Terminal Server.*

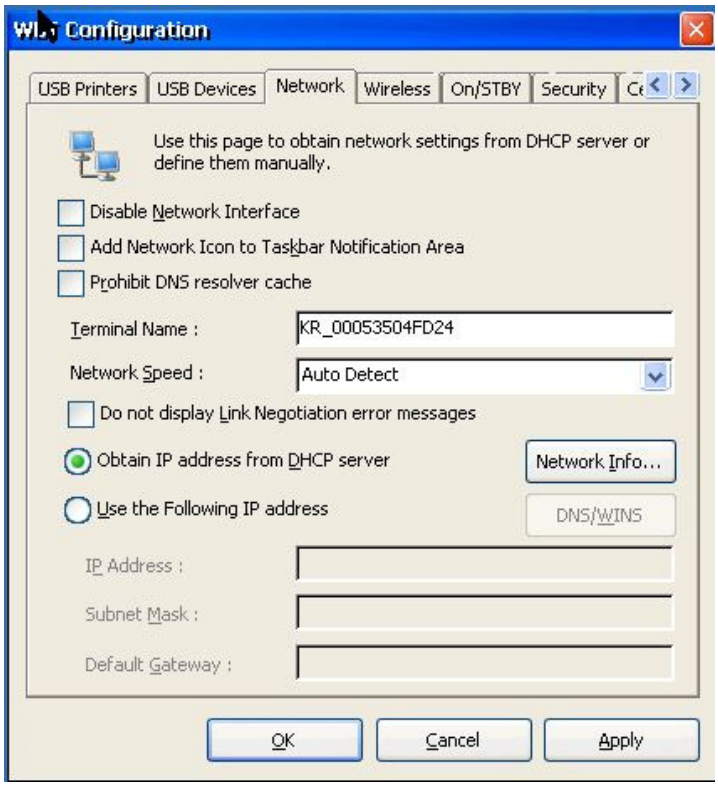
1.7 Enable Storage Mapping in ICA Session

- From WBT Setup choose the Plug-ins Tab. Configure the Citrix ICA Connection plug-in properties by choosing the plug-in and pressing Configure button.
- Storage mapping requires both server and client side configuration. On the client, the appropriate storage device from the USB Storage section of the USB Devices dialog should be enabled.
- Check the Enable connection to USB Storage devices
- Click the OK button
- Enable storage mapping support in the Citrix Server.



Network Tab - Setting the Network Connections

The Network Tab provides an interface for TCP/IP property settings. The Network tab is used to set network settings such as IP address and nameservers definitions (DNS & WINS) and to define terminal name.



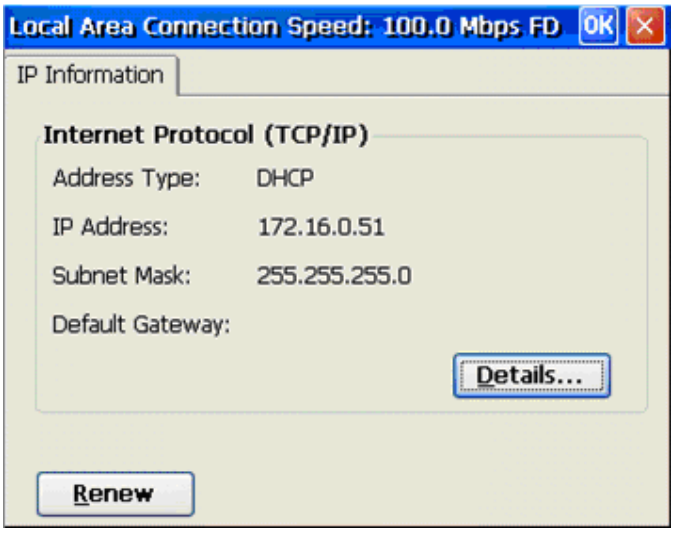
1 Disable Network Interface (for dialup users):

This option eliminates network interface for Dialup users for whom all connection parameters are defined through the Dial up connection properties.

2 Add Network Icon to Taskbar Notification area:

Marking this checkbox results in a Network Icon displayed in the System Tray indicating the network link status (connected / not connected).

Double clicking the Network Icon will prompt the IP Information dialog, displaying general TCP/IP properties.



- Renew: Triggers an IP renewal.
- Details: View advanced TCP/IP properties (e.g. MAC Address / DNS Info / WINS Info…etc).

3 Prohibit DNS Resolver cache:

By default information received from DNS is cashed on the device. Enable this option to prevent cashing of that information on the device. In some cases System administrators balance the load on their servers by listing several IP addresses under the same name, in order to enable this option you have to mark this checkbox.

- Terminal Name: Define a NetBIOS name in the text box. The Terminal Name is the name to be used to identify the device.
- Network Speed: Using the Network Speed combo box select the appropriate network. LAN interface speed settings (Auto / 100 Half Duplex…etc).

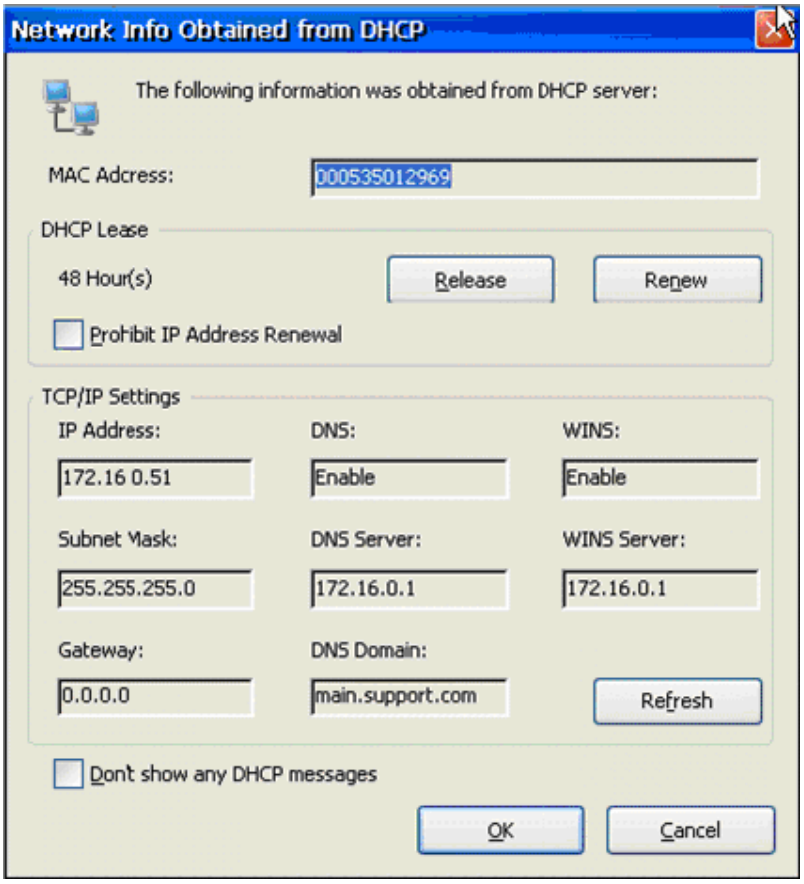
4 Obtain IP address from DHCP server / Use the following IP address:

IP address can be obtained either manually by entering the IP address → Subnet Mask and Default Gateway. Or dynamically through the DHCP by selecting the radio button of Obtain IP Address from DHCP.

5 Network Info:

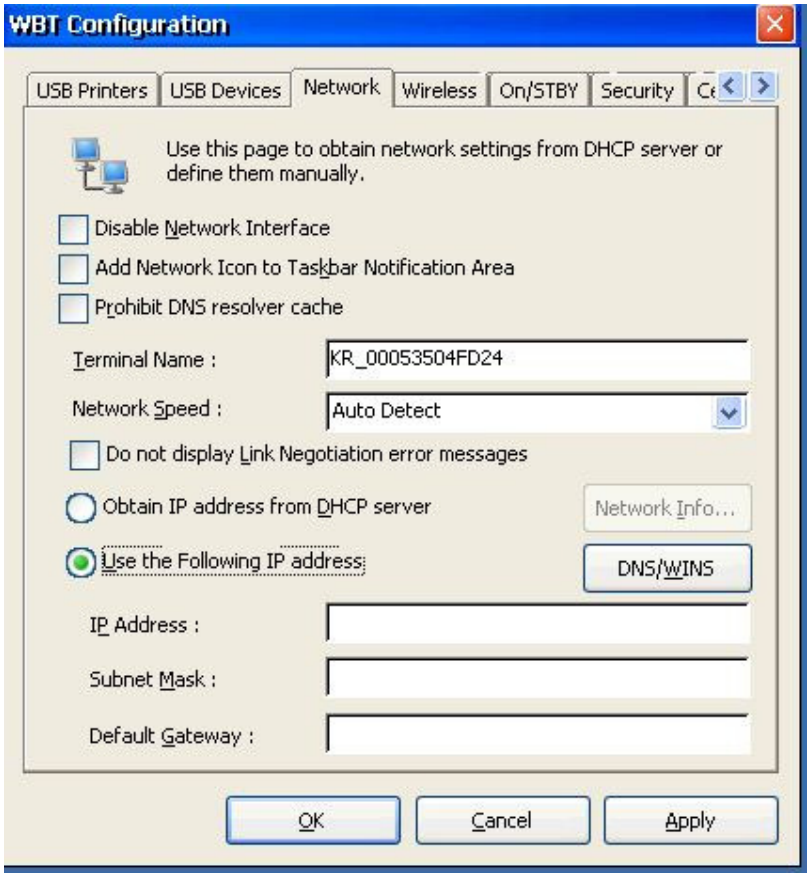
View the device's network information, such as MAC address and TCP/IP settings.

- Release: Released IP Address currently used.
- Renew: Obtains a new address through the DHCP server.
- Prohibit IP Address Renewal: Prohibit Users from manually renewing IP address.
- Don't Show any DHCP massages: In some cases due to slow network performance the DHCP handshake takes longer than default. As result, an event is displayed on screen. Enabling this option, through Network Tab Network Info prevents the device from notifying users of any DHCP events. Please note that hiding DHCP events may impact network troubleshooting outcomes.



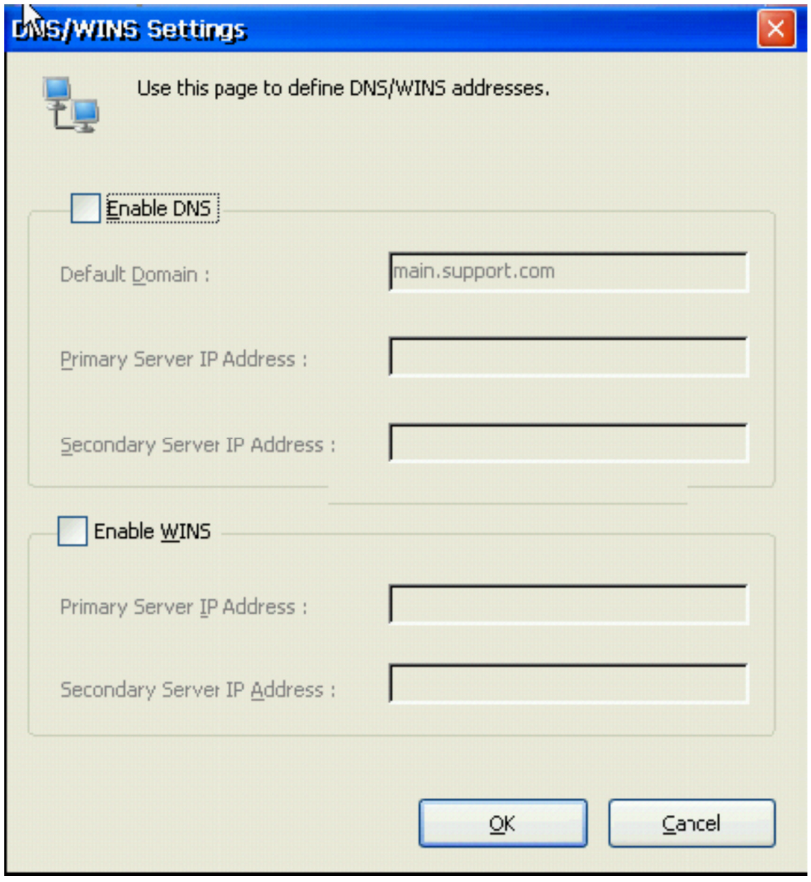
6 Manual IP Address:

Once the Radio Button of Use the Following IP Address is marked, you will need to manually define network properties for the device.



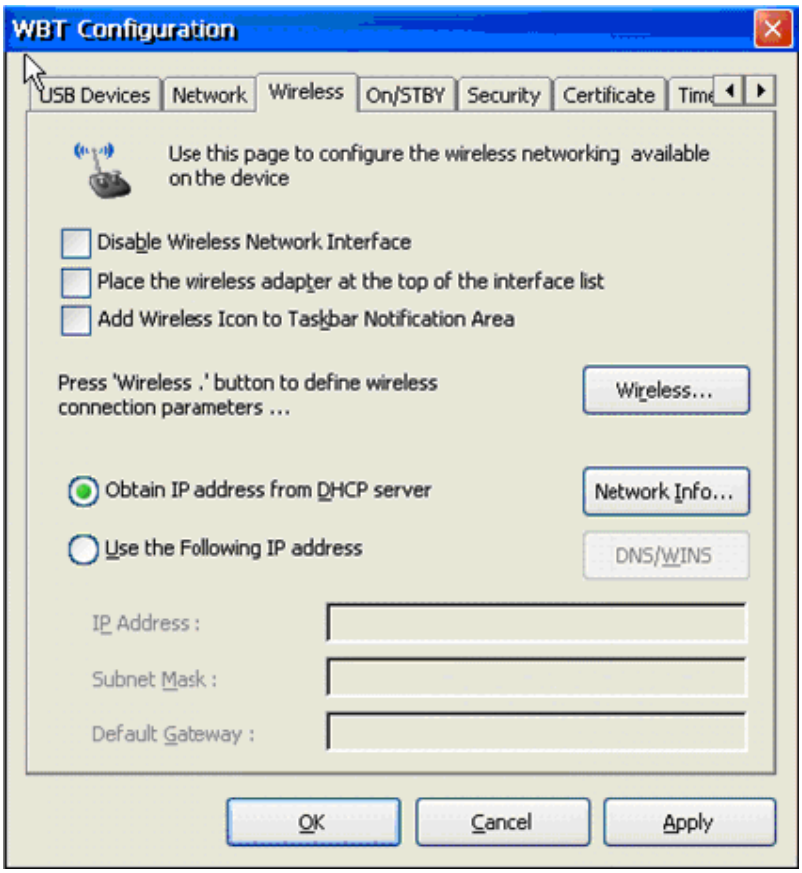
- Specify the IP Address, Subnet Mask and Default Gateway in their respective Input Fields.

- Press the DNS/WINS button than mark relevant checkbox and insert the information to the relevant Input Fields:
  - Default domain
  - Primary Server IP address (for DNS and WINS)
  - Secondary IP address (for DNS and WINS)
  - OK to return to the Network Tab with the changes made or Cancel to return without keeping the changes.



Wireless tab

Chip PC supports a wireless USB NIC in image 6.5.3.



1 Disable Wireless Network Interface:

Disables the wireless NIC.

2 Place the wireless adapter at the top of the interface list:

Both NICs are active by default (if they're both connected) and the embedded adapter has priority over the wireless adapter. This option lets you set the wireless adapter as the default network adapter.

3 Add Wireless Icon to Taskbar Notification Area:

The Icon is an image of 2 computers side by side, to view this icon, or any other icon, the System Tray area must be enabled.

To enable it go to Start -> Settings -> desktop, access the Taskbar tab and select the option "Show System Tray".

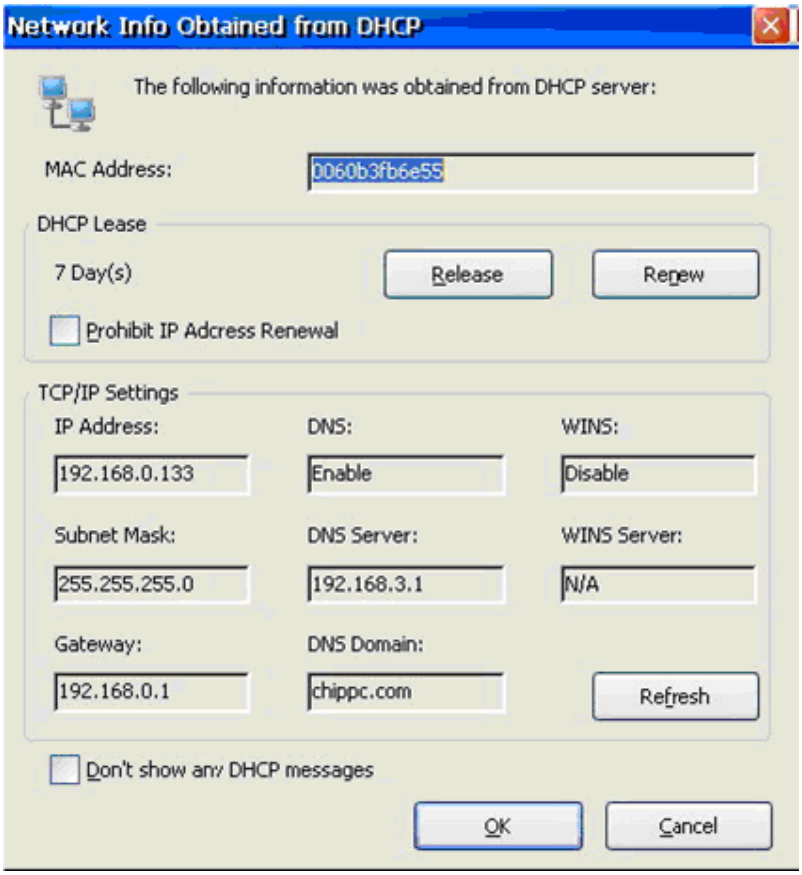
4 Obtain IP address from DHCP server:

IP address and other parameters can be obtained from a DHCP server.

Click the "Network Info…" button to view that information. Through this interface you can:

- Release and Renew the IP address
- Prohibit IP Address Renewal
- Refresh the information displayed

Prevent DHCP messages from being displayed.



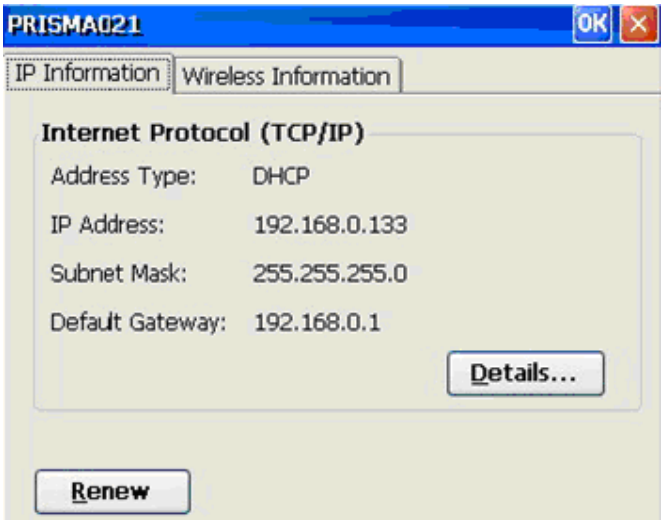
5 Use the Following IP address:

Manually set network parameters instead of using a DHCP server.

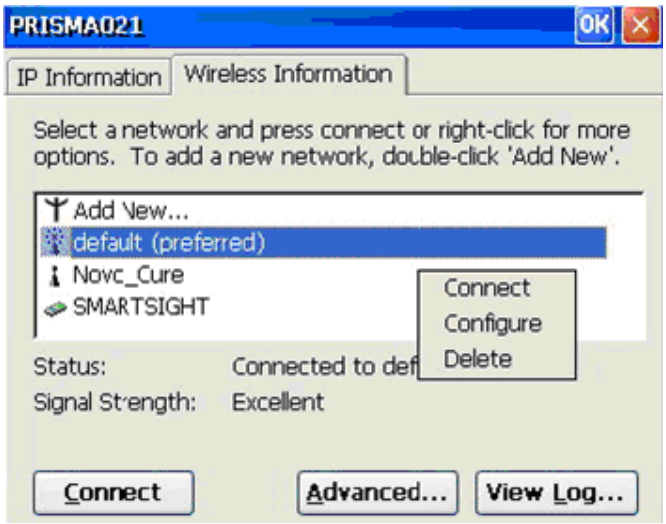
6 The "Wireless" button:

Define the wireless connection parameters.

- IP Information: Provides information regarding the TCP/IP protocol, as shown in the image above.



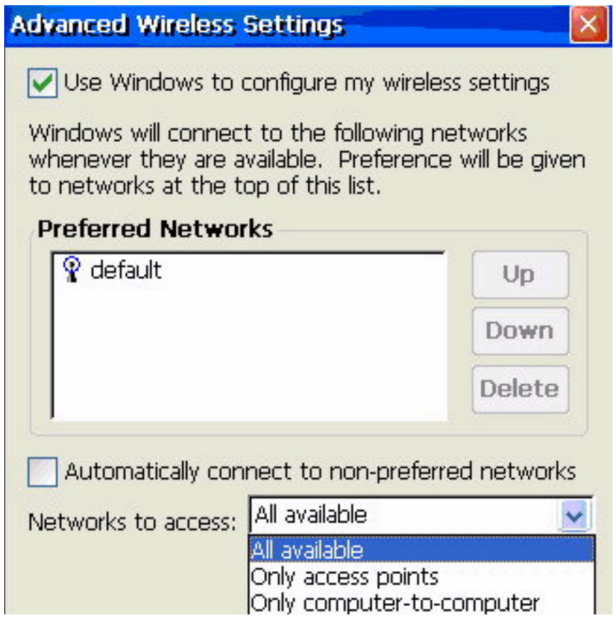
  - Renew: Renew IP address.
  - Details: Provides more details on the network connection.
- Wireless Information:



  - Select a network connection from the list box and click Connect (items are automatically detected and added to list box).

- Right-click a connection for more options: Connect, Configure, Delete. Choosing Configure will open the Wireless Network Properties dialog (also opens when creating a new connection).
- To create a new connection, double-click Add New the Add new wireless network dialog will open. Enter all the necessary information (this section is MS standard).

- Advanced: Opens the Advanced Wireless Settings dialog, set the priority of the connections, as shown below.

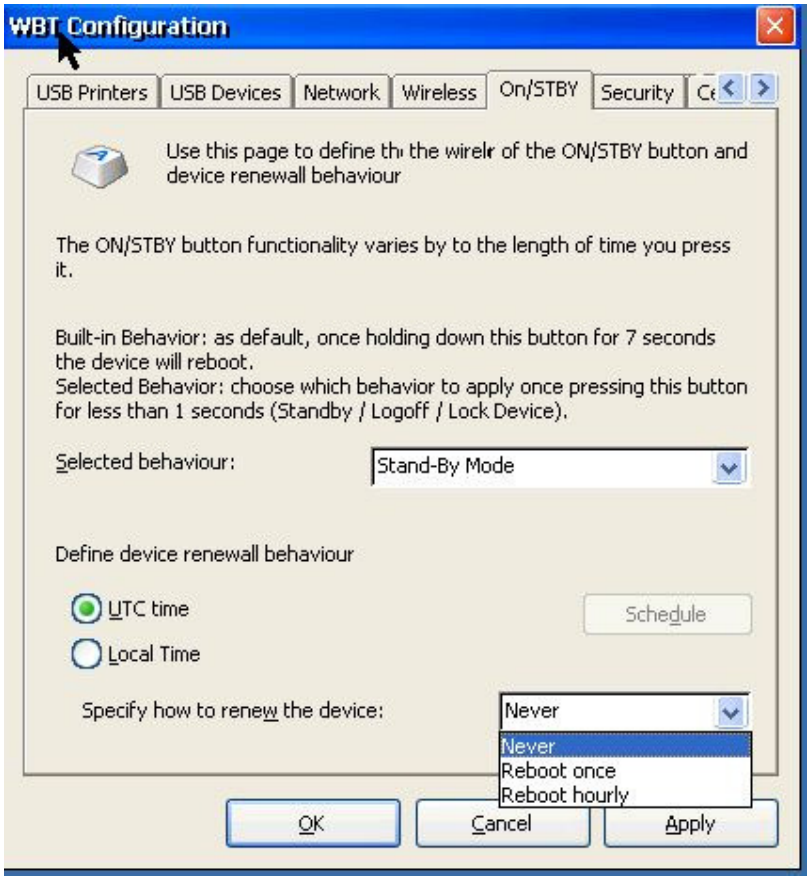

Advanced Wireless Settings
Use Windows to configure my wireless settings
Windows will connect to the following networks whenever they are available. Preference will be given to networks at the top of this list.
Preferred Networks
default
Up
Down
Delete
Automatically connect to non-preferred networks
Networks to access:
All available
All available
Only access points
Only computer-to-computer

- View Log: Opens the Wireless Networking Log, which provides more information.

NOTE *Note: The wireless driver may be compatible with other wireless devices, such as US Robotics USR805422. However, there is no guarantee that it will work properly on any other devices not purchased from Chip PC.*

On/STBY Tab

The ON/STBY tab enables user to define which behavior will apply once the ON/STBY button is pressed for less then 1 second. If the ON/STBY button is pressed for more than 1 second the device will be rebooted.


WBT Configuration
USB Printers
USB Devices
Network
Wireless
On/STBY
Security
Use this page to define th the wirelr of the ON/STBY button and device renewall behaviour
The ON/STBY button functionality varies by to the length of time you press it.
Built-in Behavior: as default, once holding down this button for 7 seconds the device will reboot.
Selected Behavior: choose which behavior to apply once pressing this button for less than 1 seconds (Standby / Logoff / Lock Device).
Selected behaviour:
Stand-By Mode
Define device renewall behaviour
UTC time
Local Time
Schedule
Specify how to renew the device:
Never
Never
Reboot once
Reboot hourly
OK
Cancel
Apply

Users can select one of four responses:

1 Stand-By Mode:

Stand-By Mode is a power saving mode that requires the user to restart the device either by pressing the reset button or by a network command.

2 Log-off:

Once pressing the ON/STBY button, the device will restart and log-off users connected to it.

3 Lock Device:

Lock Device will force users to enter their credentials once the device was restarted using the ON/STBY button.

4 N/A:

Standby Mode is a power saving mode into which a device enters as a result of user command (pressing the ON/STBY button or selecting STBY from the shutdown menu) or power failure. Devices in Standby Mode can be either awakened by a network command or by a user command pressing the ON/STBY button. In scenarios where devices are placed in unreachable locations (e.g. under tables…etc), disabling the Standby Mode might be required.

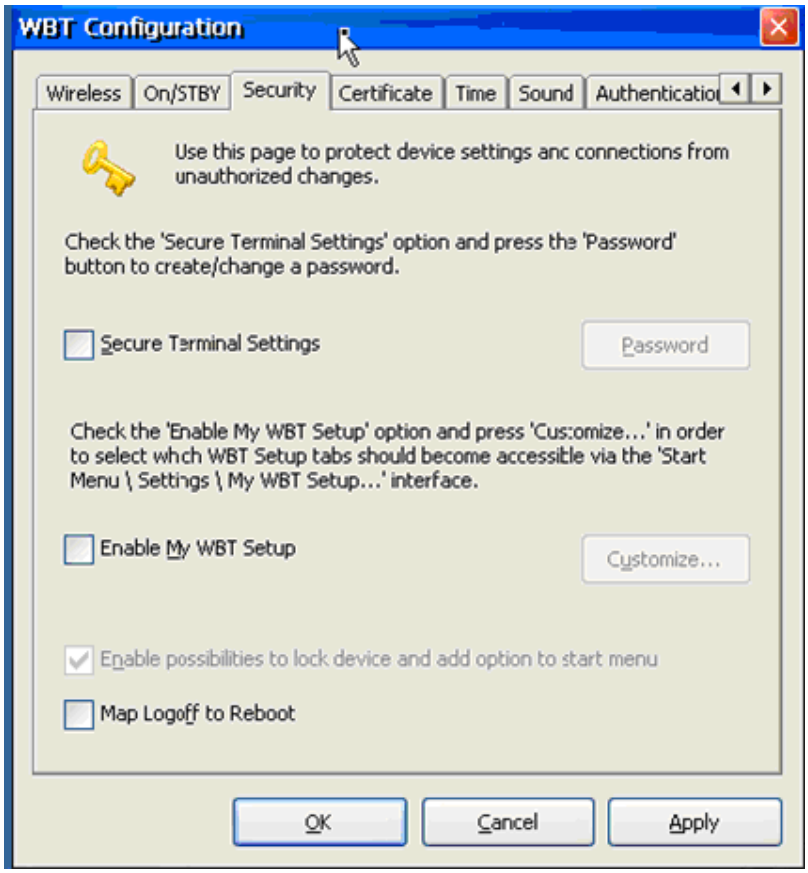
NOTE *Disabling the Standby Mode sets the device status as always-on.*

5 Device Auto Restart Schedule

- UTC Time: The process will be done according to the UTC time Zone
- Local Time: The process will be done according to Local time

Security Tab

The Security tab is used to protect the device configuration and connections from changes made by the user.


WBT Configuration
Wireless
On/STBY
Security
Certificate
Time
Sound
Authentication
Use this page to protect device settings anc connections from unauthorized changes.
Check the 'Secure Terminal Settings' option and press the 'Password' button to create/change a password.
Secure Terminal Settings
Password
Check the 'Enable My WBT Setup' option and press 'Customize...' in order to select which WBT Setup tabs should become accessible via the 'Start Menu \ Settings \ My WBT Setup...' interface.
Enable My WBT Setup
Customize...
Enable possibilities to lock device and add option to start menu
Map Logoff to Reboot
OK
Cancel
Apply

1 Secure Terminal Settings:

Set a password to secure the entire WBT Setup environment.

2 Enable My WBT Setup:

Define limited access options to some of the WBT Setup tabs according to user needs.

3 Publishing Device Access Shortcuts:

My WBT Setup can be used to provide a custom “slim” WBT Setup Environment to users who require access to parts in the WBT other than the default device shortcuts.

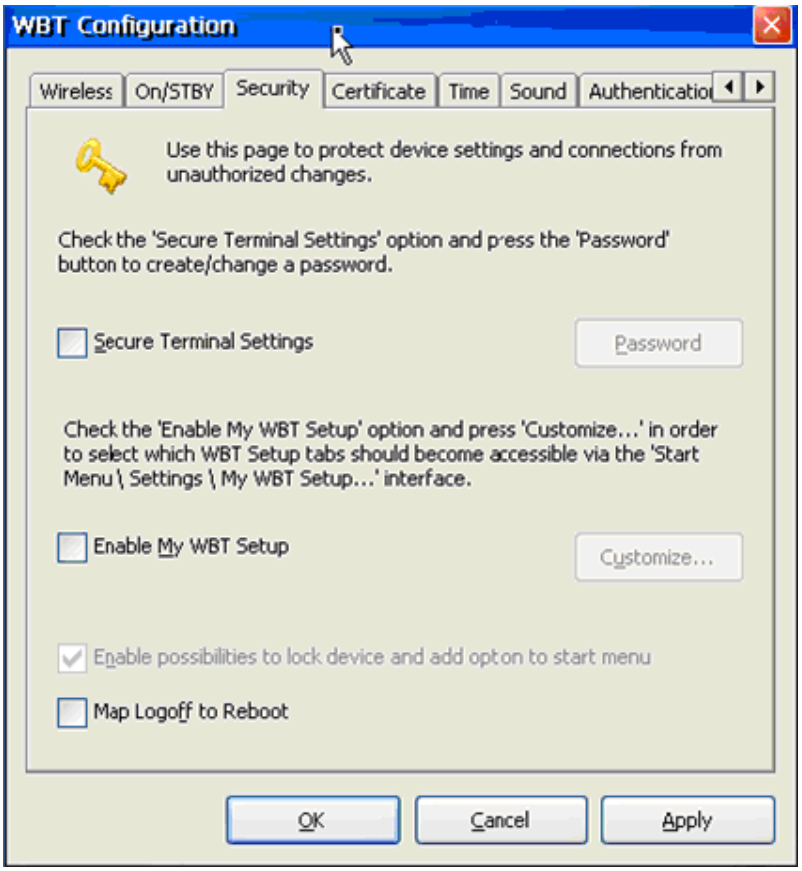
The My WBT Setup item is accessible from the Start Settings menu as a custom made WBT Setup interface.

3.1 Scenario:

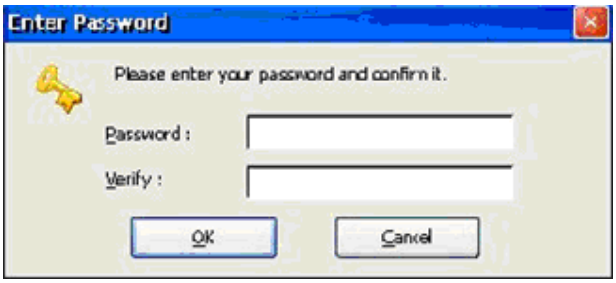
Some users are to be given access only the Input, Display, Printers, Time and Sound tabs and denied access from all other WBT Setup tabs.

3.2 Actions Needed:

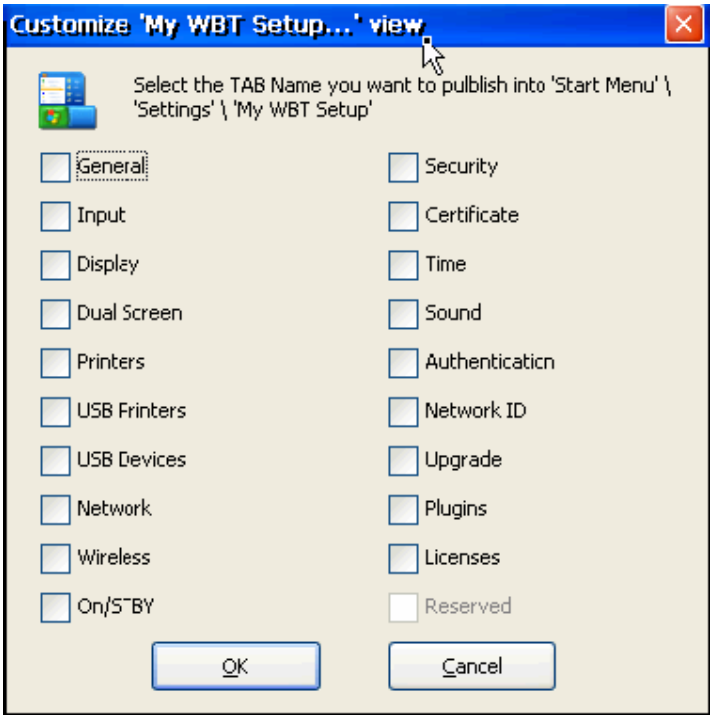
- Go to Start → Settings → Device
- Through the Security tab mark the Secure Terminal Settings checkbox.
- Press the Password button


WBT Configuration
Wireless
On/STBY
Security
Certificate
Time
Sound
Authentication
Use this page to protect device settings and connections from unauthorized changes.
Check the 'Secure Terminal Settings' option and press the 'Password' button to create/change a password.
Secure Terminal Settings
Password
Check the 'Enable My WBT Setup' option and press 'Customize...' in order to select which WBT Setup tabs should become accessible via the 'Start Menu \ Settings \ My WBT Setup...' interface.
Enable My WBT Setup
Customize...
Enable possibilities to lock device and add option to start menu
Map Logoff to Reboot
OK
Cancel
Apply

- Enter a Password and Verify



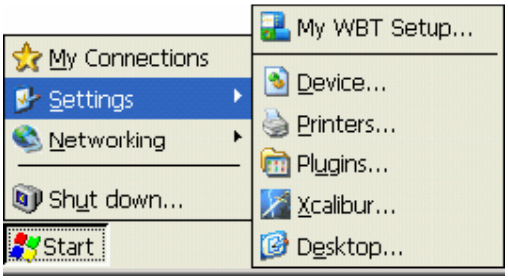
- Click OK to finish
- Check the Enable My WBT Setup checkbox
- Press the Customize button
- Select the Input, Display, Printers, Time and Sound tabs
- Click OK to close all dialogs and restart the device



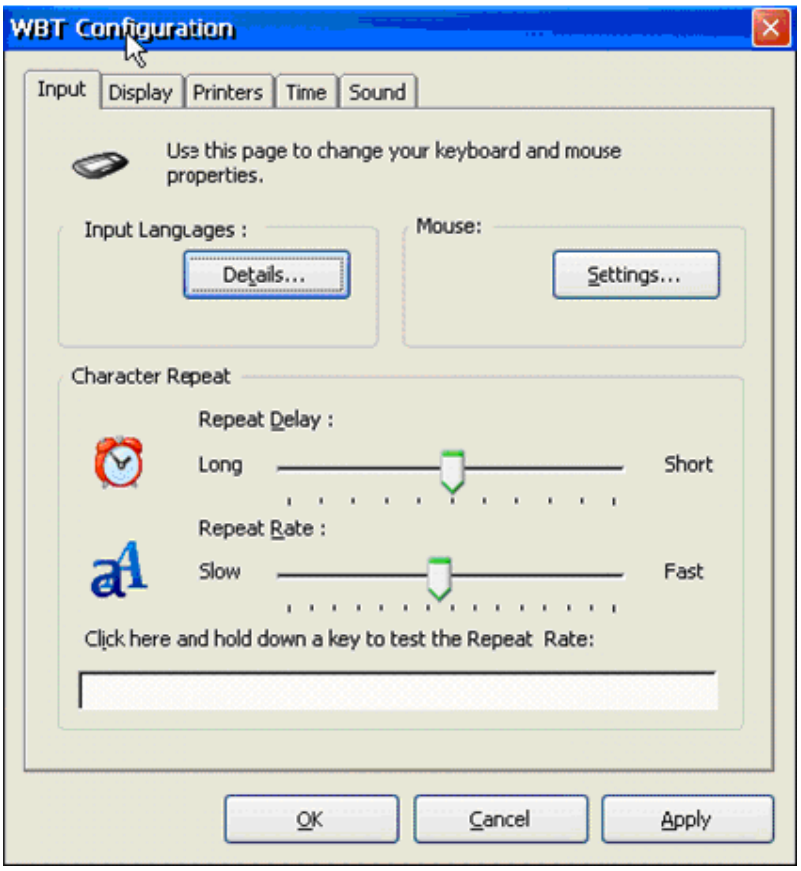
3.3 Results:

Once the device is restarted go to Start → Setting menu, the Default Device shortcut has become password protected.

The “My WBT Setup” item is now available.



When selected, a custom WBT Setup is displayed showing only the Input, Display, Printers, Time and Sound tabs.



4 Enable possibility to lock device and add option to start menu:

By enabling this option users will be able to lock their device, making sure that only the current user will be able to unlock the device.

NOTE *This option can only be used with Xcalibur domain authenticator license.*

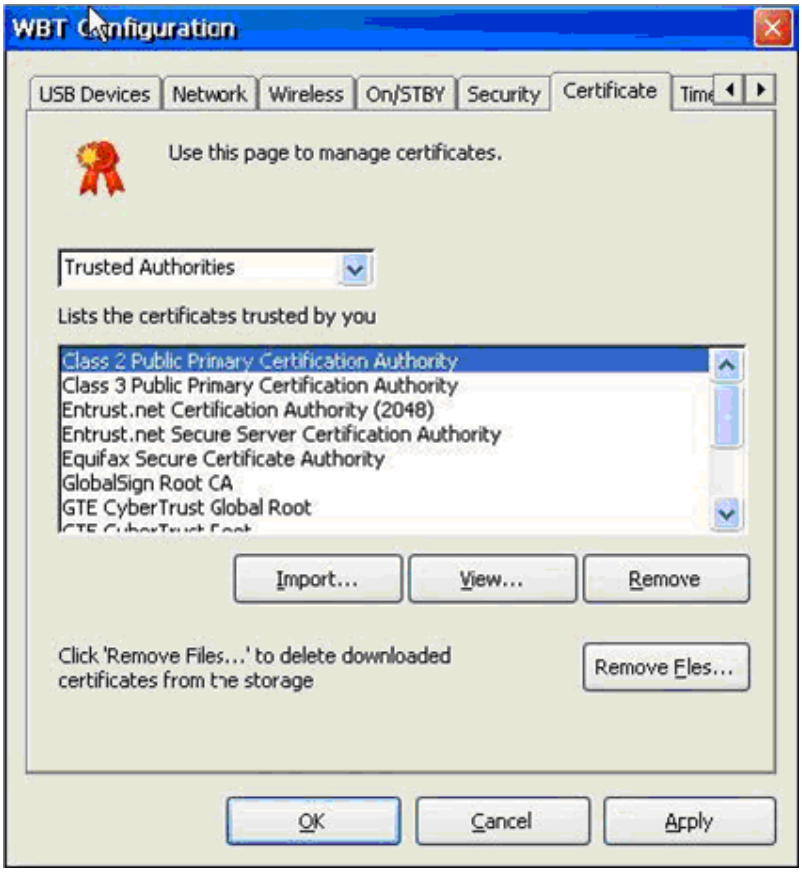
5 Map Logoff to reboot:

In order to enable applications that run on startup, each time a user logs-off the client will reboot.

Certificate Tab

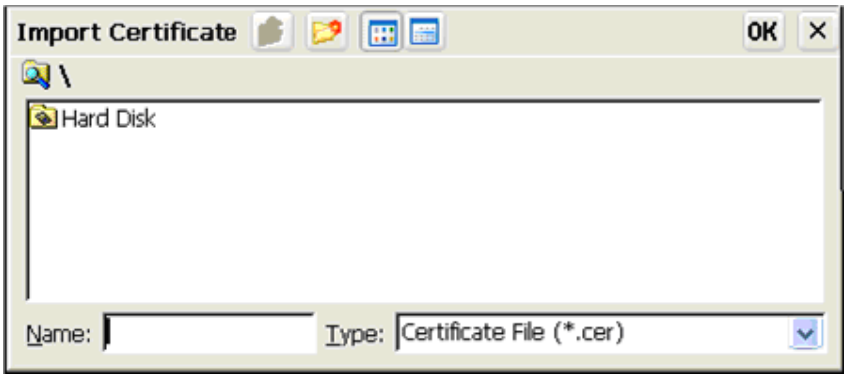
Use this tab to manage the certificates installed on your device. Define your certificate authorities and install or remove certificate on the device.

Chip PC devices use SSL encryption for different connections include connection to Xcalibur Global management software.



1 Import: Import New Certificate.

Click the Import button to open the Import Certificate Window



- Choose from storage device or enter the name of the directory in which the certificate is stored on.
- Click the OK button.

View:

View Certificate properties.

Remove:

Click the Remove button to delete a Certificate.

Remove Files:

Click to delete all certificates that are kept in storage.

Time Tab

The Time tab provides the interface for time property settings. Time settings include two main fields: Time Zone and Real Time Information.

1 Time Zone

Time Zone settings affect the Session Time which reflects the date and time displayed to the user through applications during a session.

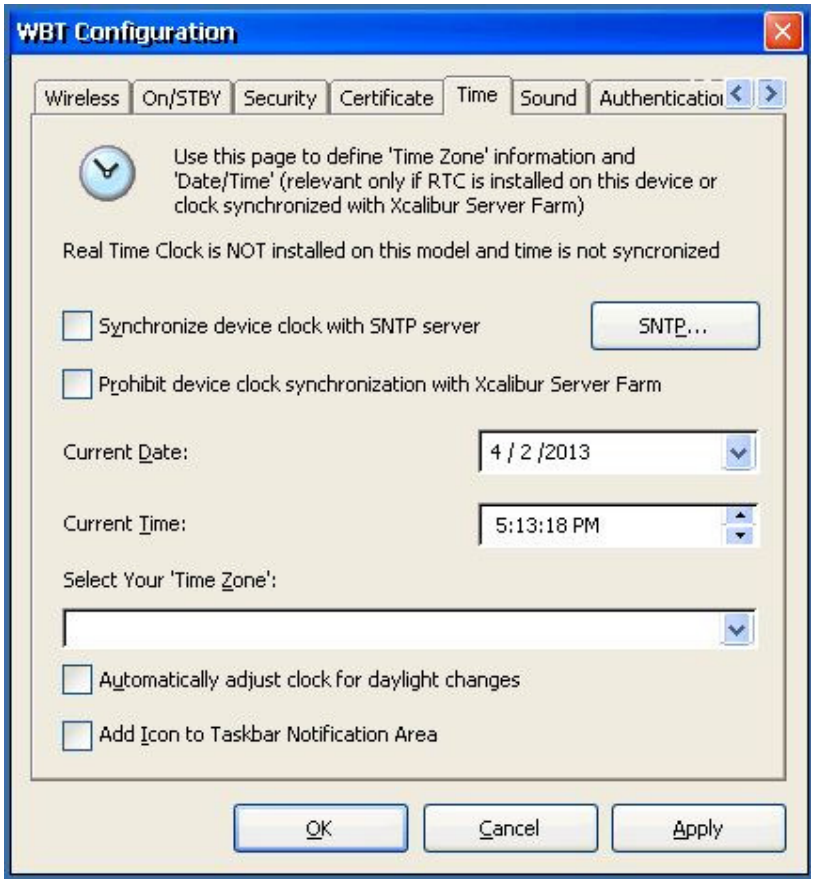
Session Time is mostly associated with calendar/journal applications (e.g. Outlook / Lotus notes…etc). Organizations with branches spread over different countries and time zones prefer users (while in a session) to see and use their local time zone corresponding to their physical location.

2 Session Time

Calculation depends on both server and client settings as described by Citrix knowledgebase document ID CTX303498:

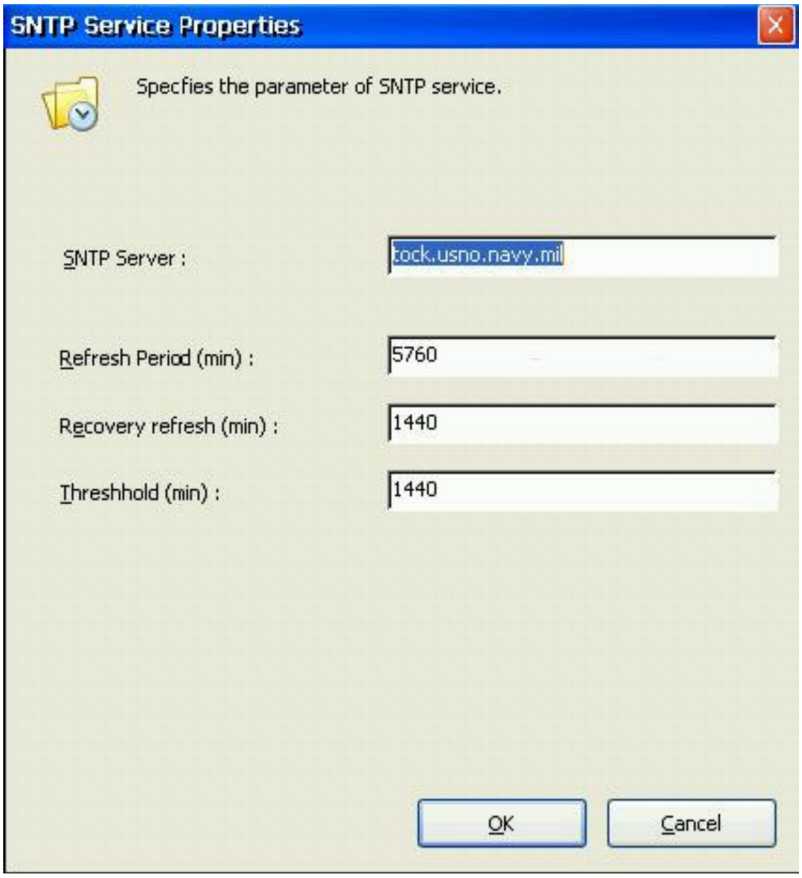
"When Client Time Zone, CTZ, is enabled, the client passes its time zone information to the server. The server obtains the clients time zone information (GMT, daylight saving, etc) and compares it with its own time zone information.

If it is different, the server stores the clients' time zone information in the registry. A time zone hook is loaded for every application running inside that client session. Those applications use the clients' time zone instead of the servers."


WBT Configuration
Wireless
On/STBY
Security
Certificate
Time
Sound
Authenticatio
Use this page to define 'Time Zone' information and 'Date/Time' (relevant only if RTC is installed on this device or clock synchronized with Xcalibur Server Farm)
Real Time Clock is NOT installed on this model and time is not syncronized
Synchronize device clock with SNTP server
SNTP...
Prohibit device clock synchronization with Xcalibur Server Farm
Current Date:
4 / 2 /2013
Current Time:
5:13:18 PM
Select Your 'Time Zone':
Automatically adjust clock for daylight changes
Add Icon to Taskbar Notification Area
OK
Cancel
Apply

NOTE *When Client Time Zone, CTZ, is disabled, the Time Zone used within a session will be the server's. In this case the client's 'Time Zone' settings will be ignored*

- Synchronize Device Clock with SNTP server: synchronize client clock with SNTP Sever, client's clock will be adjusted according to SNTP + local time zone defined in the client.
- Prohibit Device Clock Synchronization with Xcalibur Server Farm: Block client from synchronizing with Xcalibur, there for the client will show it's own time.
- Select your time zone: Choose the time zone the client is in, important for synchronization with Xcalibur (if client is not in the same time zone).
- SNTP: Click button to define and configure SNTP server synchronization.



Sound Tab - Setting the Sound Properties

The Sound tab is used to set the sound properties of the device.

Mute Mic:

Mark the Mute Mic checkbox to disable the Microphone connected to the device

Volume Control Sliders:

Adjust the volume of the Device.

Mute Line Out:

Mark the Mute Line Out checkbox to mute the sound on the device completely

Volume control sliders:

Control the volume settings of the device

Events:

Mark checkbox to enable events sound

Application:

Mark checkbox to enable sound from applications

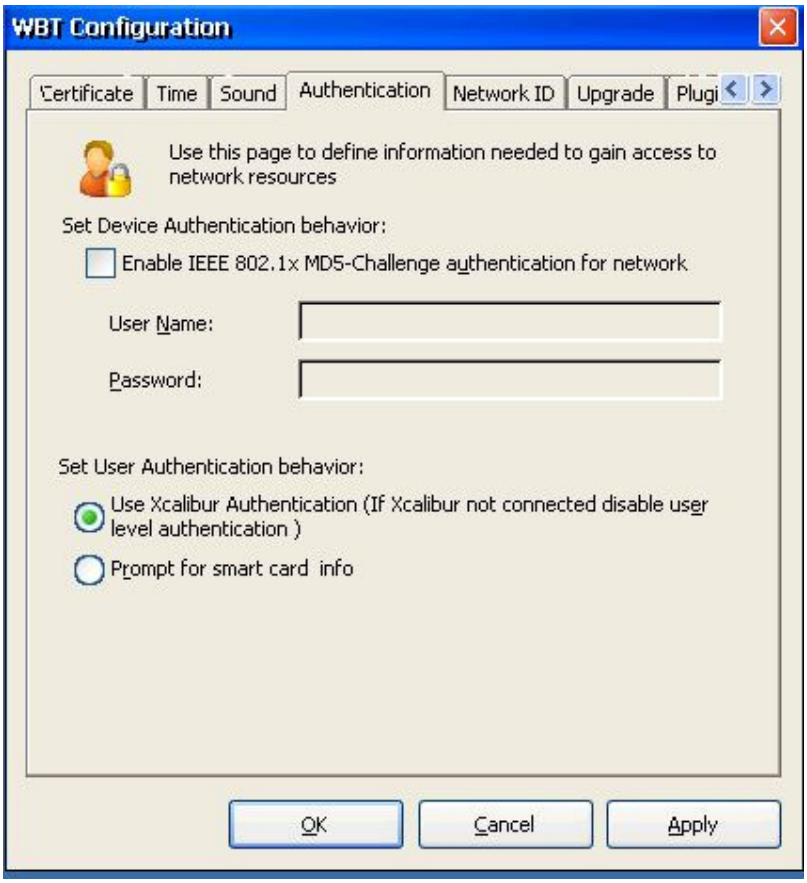
Authentication Tab – Configure the device authentication settings

The Authentication tab centralizes all authentication settings.

1 Built-in Authentication

Devices running Image Version 7.0.X have built-in user authentication mechanisms to be used in the following ways:

- Secured device access.
- Obtaining user-based settings from Xcalibur Global Domain Authenticator.
- Transparently access network resources.



2 Use Xcalibur Authentication:

Rely on authentication by Xcalibur Global.

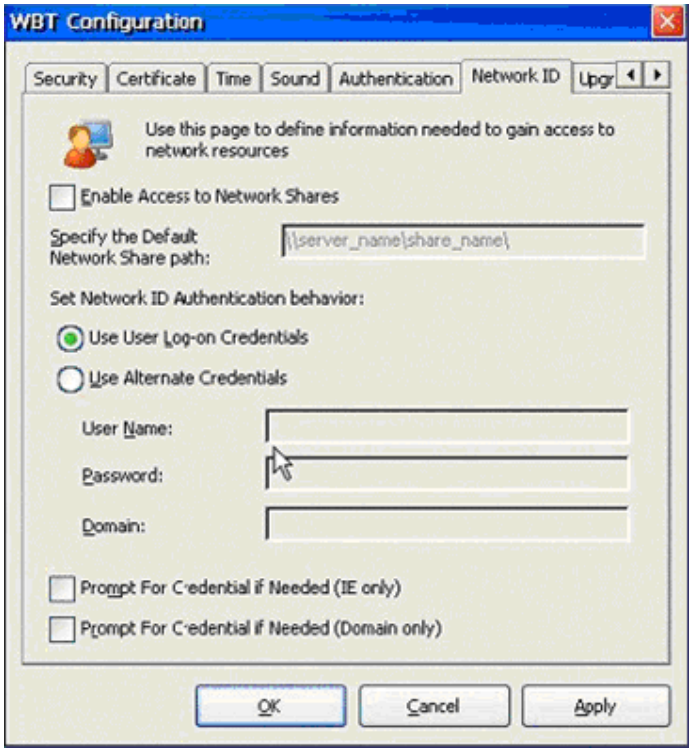
3 Prompt for smart card info:

Authenticate local user using smart card before allowing access to the device.
At this moment this option is not functional.

Network ID Tab

Image version 7.0.x has various built-in capabilities of network access. Devices can access network stores for file / image / Plug-in / license downloads. A network store can be a predefined Shared Folder, an FTP Directory, a Network Database, an external USB Storage or other.

User credential provided during logon or predefined under the Network ID tab are used in order to obtain access privileges to the path specified in the Network ID tab.



1 Enable Access to Network Shares:

Once specifying a UNC path to a network share (\\Servername\Sharename\) downloading Plug-ins and License files becomes possible by selecting the Use Network Share option during Plug-ins / License installation. (See Plug-in / License installation instructions for further details).

The path (either UNC or Local) specified via the Network ID tab is considered to be the only-default path accessible by the device for license / Plug-in installations.

2 Set Network ID Authentication Behavior:

Network ID authentication behavior determines how the device performs userlevel authentication while accessing the Default Shared Folder.

Specify whether the device should use the Logged-On user credentials as set through the Authentication Tab, or other alternative credentials.

2.1 Prompt for Credentials if Needed (IE Only):

Triggers the devices to prompt for alternate user credentials, this can be useful for example when connecting through a proxy server, the user might not have had to log on to a domain controller however the proxy server will need to receive credentials in order to pass the user through.

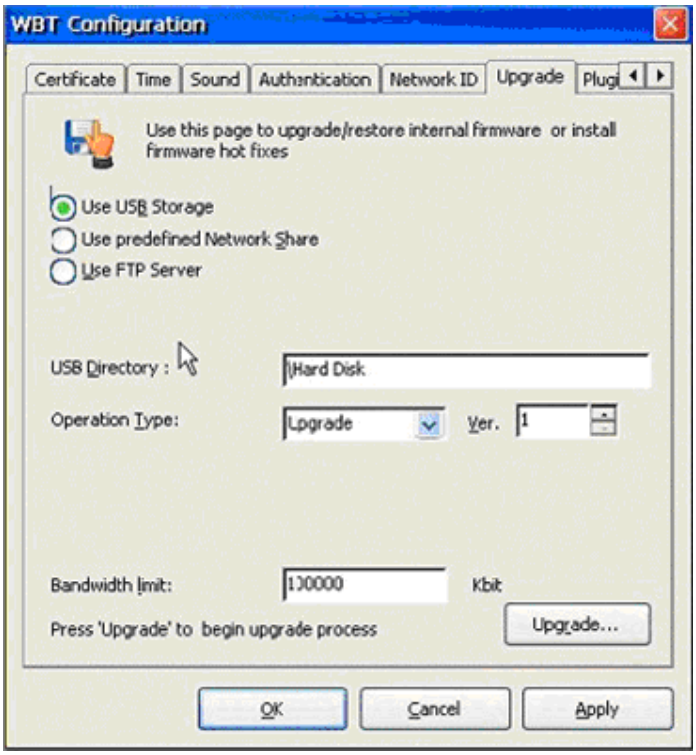
2.2 Prompt for Credentials if Needed (Domain Only Selecting the):

Triggers the device to prompt for alternate users credentials incase the ones defined do not match while browsing for a network resource (e.g. Shared Folder).

NOTE *In case Prompt for Credentials if needed… options are not selected. No error message or prompt will be displayed to users in logon failure events.*

Upgrade Tab - Setting Software Upgrade Properties

The Upgrade tab is used to set and configure the sources for Upgrade/ System restore / Hot Fix installations.



There are three possible sources of Upgrades/ System restore / Hot Fix:

1 USB Storage:

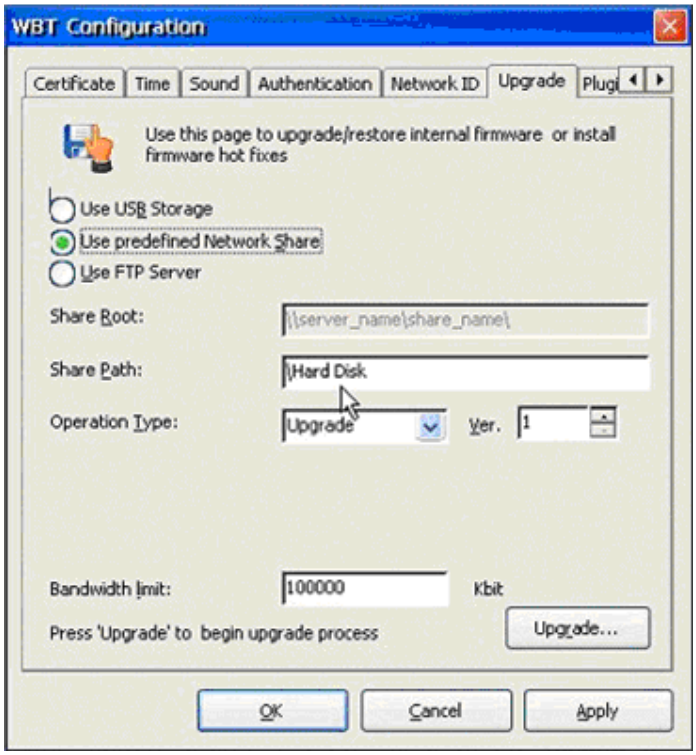
Using this option will enable user to upgrade the device image from a USB Storage device. In order to use this option you have to check the Enable Connection to USB Flash Devices on the USB Devices of the WBT dialog (see USB Devices Tab p. 46).

- Type the location of the file on the USB device starting with \Hard Disk as root
- From the Operation Type combo select the appropriate Operation (Upgrade, Hot Fix, System Restore)
- Set the Bandwidth Limit
- Press Upgrade to start the upgrade process

2 Predefined Network Share:

Users can use this option to load an upgrade package from a predefined network share. In order to enable this option you have to check the Enable Access to Network Shares on the Network ID tab of the WBT dialog (See Network ID Tab p. 68).

- Type the default network share path in the following manner: \\Computername\Share name\
- In the Upgrade tab check the Use Predefined Network Share checkbox
- Define the location of the package you wish to install in the Share Path text box (Folder\Sub-Folder)
- By using the Operation Type combo box define the type of operation you wish to perform
- Configure the Bandwidth Limit
    - Press Upgrade to start the upgrade process



3 FTP Server:

Type the FTP Server Name and Directory in the respective Input Boxes.

By using the Operation Type combo box define the type of operation you wish to perform

- Define access information to FTP server in the FTP USER ID and Password Input Boxes.
- Configure the Bandwidth Limit
- Press the Upgrade button to start an upgrade process, following the instructions to complete it successfully.

Plug-ins Tab

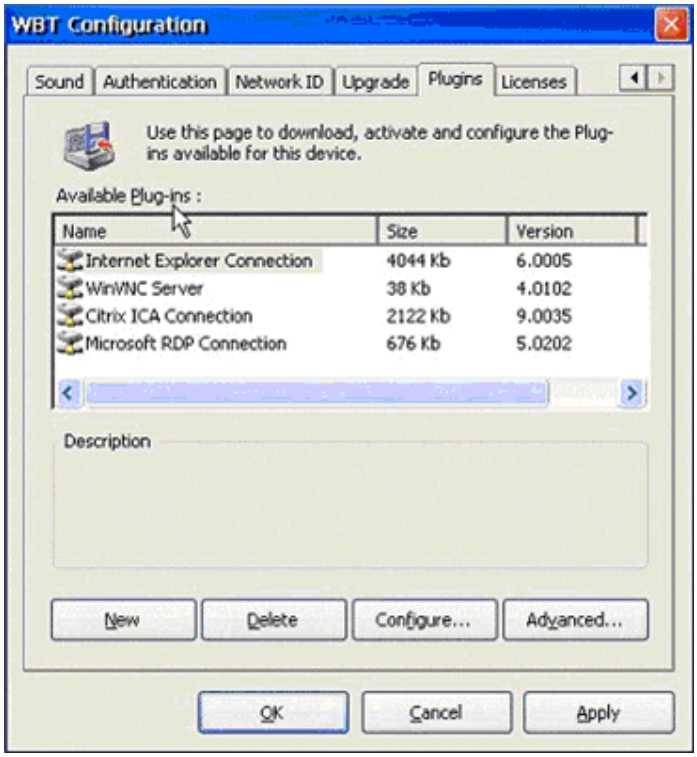
Plug-ins are software add-ons that can be installed on Chip PC thin client devices.

Chip PC thin clients are scalable to integrate a variety of software components such as print optimization tools, security related plug-ins, management utilities etc'.

The Plug-ins tab is used to download, activate and configure different software Plug-ins to provide your device with extra functionality and customization.

NOTE *In some cases one must purchase and install a license in order to be able to use certain plug-ins and manage device with Xcalibur Global (see section on Licensing Tab).*

The Available Plug-ins window provides a display list of the downloaded plugins, their size and software version.



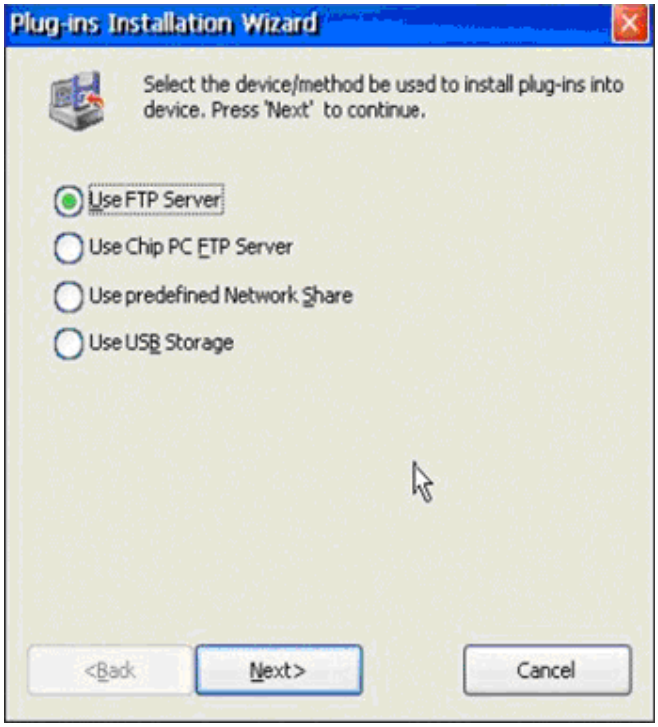
By selecting a plug-in and pressing the Configure button you will be able to access advanced configuration options on the selected plug-in.

See chapter 9 of this document for an explanation regarding advanced configuration options of each plug-in.

1 Downloading a New Plug-in

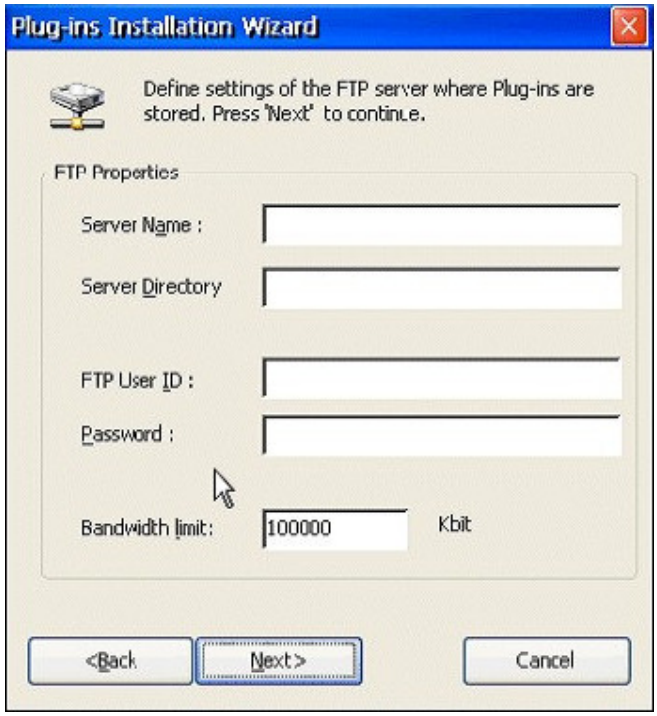
To download a new plug-in, click the New button (in the Plug-ins tab) and follow the instructions in the Plug-ins Installation Wizard. Plug-ins can be downloaded from FTP Server, Chip PC FTP Server, Network Share and USB Storage device.

Define the source from which you want to load the new plug-in:

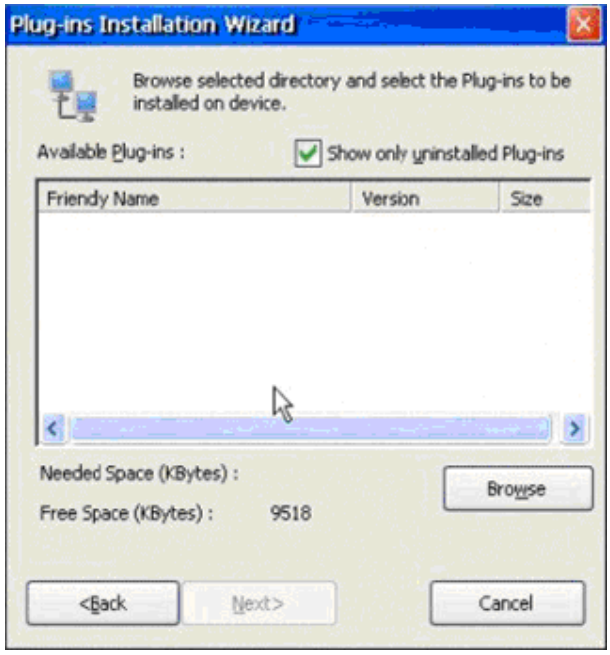

Plug-ins Installation Wizard
Select the device/method be used to install plug-ins into device. Press 'Next' to continue.
Use FTP Server
Use Chip PC FTP Server
Use predefined Network Share
Use USB Storage
<Back
Next>
Cancel

2 Use FTP Server:

- Type the FTP server parameters and click on Next (Enter the complete path to the folder location)

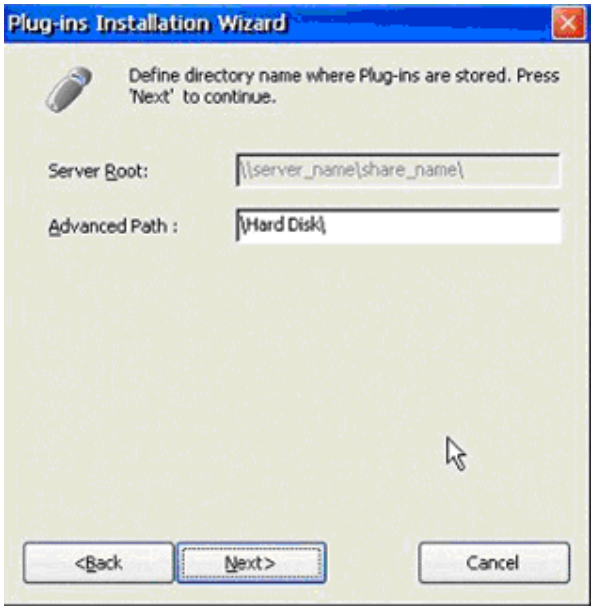


- Select the plug-in you wish to install and click on Next



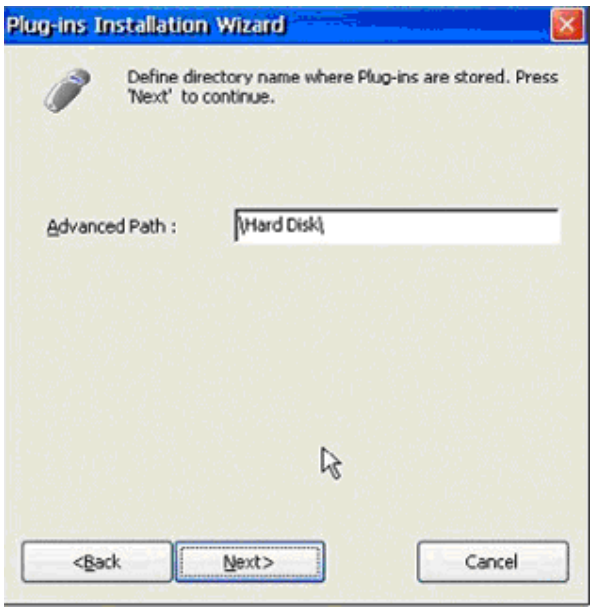
- Mark the Show only uninstalled Plug-ins checkbox to view uninstalled plug-ins
- You can use the Browse button to find the plug-in inside the FTP server
- Click on Install and read installation status in the log-file box. When installation is over, press Finish.
- The newly installed Plug-in will appear in the Plug-ins list in Plug-Ins Tab. mark the checkbox on its left side to activate it.

- Use Chip PC FTP Server:
  Use this option to download the XPI directly from the Chip PC FTP server.
  In order receive password and user name to access Chip PC FTP server contact Chip PC support department.
  Configure the following dialogs as described on the previous section.
- Network Share Download:
  - Predefined Shared Folder can be used as a Plug-in installation source.
  - Once running the Plug-in Installation Wizard, select the Use Predefined Network Share option to browse the Default Shared Folder for Plug-in files. This causes the device to display and download Plug-in files placed under the path (UNC) specified under the Network ID tab.



  - Click on Next
  - Select the plug-in you wish to install and click on Next
  - Mark the Show only uninstalled Plug-ins checkbox to view uninstalled plug-ins
  - You can use the Browse button to find the plug-in inside the FTP server
  - Press Install and read installation status in the log-file box. When installation is over, click Finish.
  - The newly installed Plug-in will appear in the Plug-ins list in Plug-Ins Tab. Mark the checkbox on its left side to activate it.

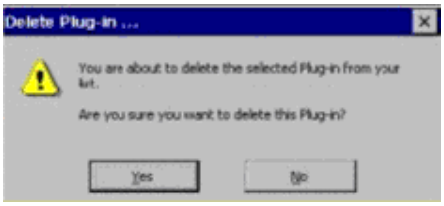
- Use USB Storage
  USB Storage devices can also be used as a source for Plug-in installation.
  - Once running the Plug-in Installation Wizard, select the Use USB Storage option to browse the USB Storage Device for Plug-in files.
  - In “Advanced path” type the complete path to plugin location, including subfolders if applicable


Plug-ins Installation Wizard
Define directory name where Plug-ins are stored. Press 'Next' to continue.
Advanced Path :
\Hard Disk\
<Back
Next>
Cancel

Follow the installation instruction as described in the previous section.

3 Deleting Plug-in

Select the Plug-in you wish to delete, press Delete and answer **Yes** to message.


Delete Plug-in ...
You are about to delete the selected Plug-in from your list.
Are you sure you want to delete this Plug-in?
Yes
No

4 Configuring Plug-in Properties

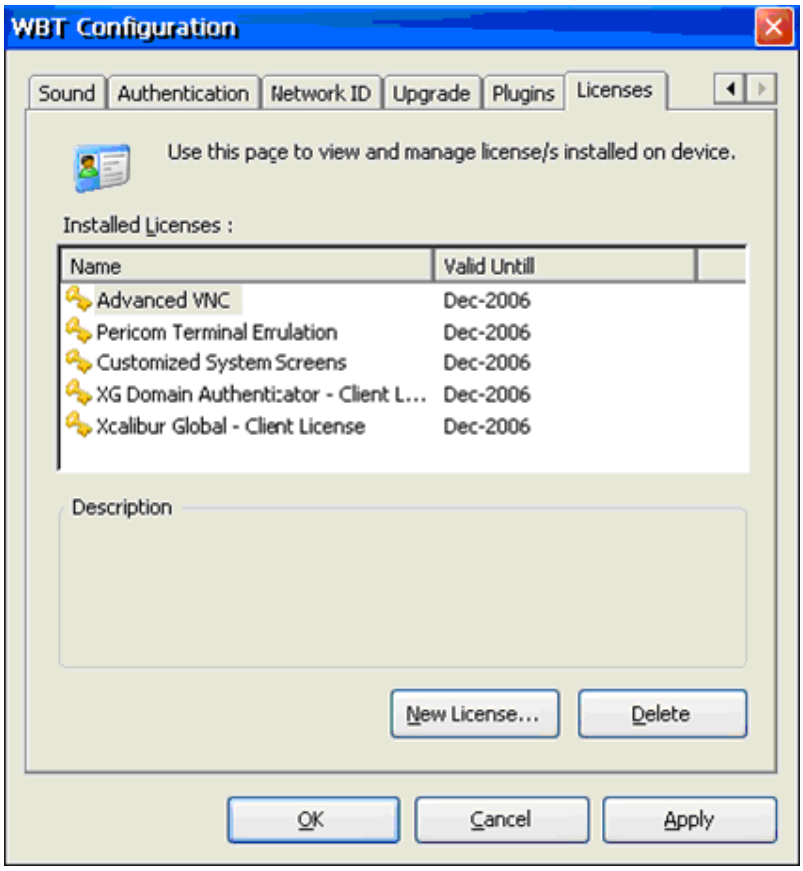
To configure Plug-in properties, mark the plug-in in the list and click the **Configure** button.

Licensing Tab

A license is required in order to enable the use of a Plug-in, Management software and specific image functionality. Unless specified, every Plug-in is license associated. Licenses can be installed before or after the Plug-ins they correspond to.

Firmware versions previous to version 7.0.x support license installation via FTP only. This means that license files could be downloaded only from a FTP server onto target devices.

Thanks to the enhanced networking and authentication capabilities embedded into firmware version 7.0.x, Default Shared Folder, and locally attached External Storage can be used as license installation sources.



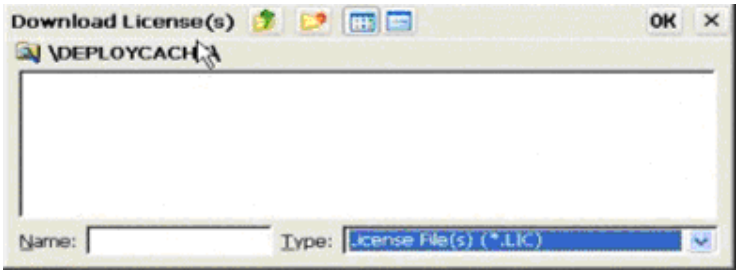
1 Installed Licenses List

After entering the WBT Setup Licensing tab, the Installed Licenses List will be displayed. This list contains the following information:

- License Name: View the names of already installed licenses.
- Valid until: View the date (month and year) each license was installed.

2 Installing a New License

- Click the New License button in the Licensing tab. Licenses can be downloaded from a Network Share or from a USB Storage device.
- In the Name text box enter your Network Share name and click OK. In order to define a network share use the Network ID tab of the WBT dialog.
- If you are using an external USB Storage device enable this option using the USB devices tab of the WBT dialog.



NOTE *In order to view license files change the Type drop list to (*.License) All licenses should be created using Chip PC Installer*

3 Deleting a License

Delete button allows the deletion of an installed license.

- Select an installed license from the Installed Licenses List and click Delete. The license will be uninstalled from device.

This page is left blank intentionally.

Chapter 5 Image 7.0.X – Connections Management

Connections are divided into two categories: Application and Network.

In image 7.0 connection management is based on the connection type.

1 Application Connections:

Application connection is a subset of parameters linked to a transport protocol and its corresponding client application (e.g. ICA / RDP …etc). Usually pointing to a terminal server or server farm or published application (or other), application connections provide users access to their working environment in form of a session.

Client applications such as RDP / ICA / I.E / Terminal Emulation etcetera are included in this category. Application connections are centrally managed via the My Connections Manager tool.

2 Network Connections:

Let devices connect to remote physical or logical networks. Network clients such as Dial-up / VPN / PPPoE etc. are included in this category. Network connections are centrally managed via the Network Manager tool.

3 My Connections

The My Connections tool is an advanced version of the 'Legacy Connection Manager' through which users are able to view, run, modify, delete and create new application connections (RDP / ICA…etc') in a centralized way.

My Connections tool is designed to present connections in two working modes Connection and Portal. Both offer great flexibility and centralization of connection management.

In order to open the Connection Manger double click on the My Connection icon on the device's desktop.

4 Connection Mode

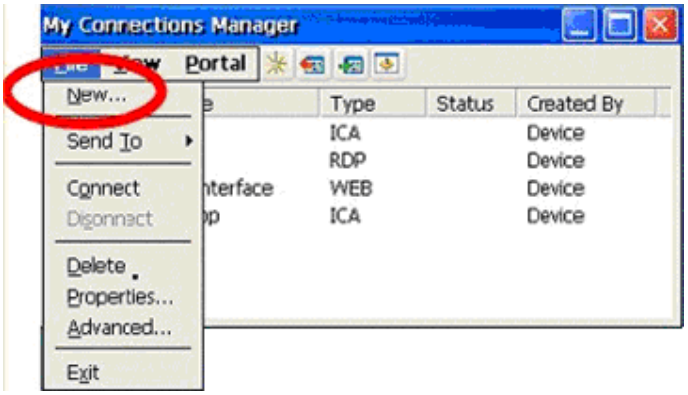
The Connection mode is a more enhanced and graphical version of the Legacy Connection Manager containing the following new features:

New Features in My Connections Manager

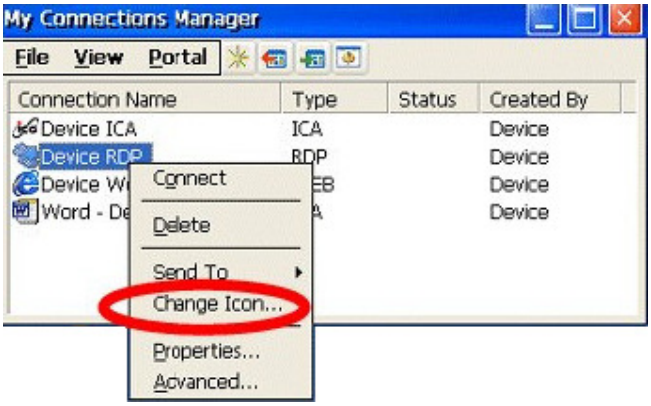
- **Connection Icon Association:** Change 'Connection' icons to reflect the application the connection points to. By browsing the built-in icon pool, administrators can replace the default connection icons to better reflect the application associated with a connection. For example replace the default RDP icon of a published Microsoft Excel application with the genuine Excel icon. Connection icons are also displayed by the session window frame even when minimized to taskbar.
- **Connection Shortcuts:** Create connection shortcuts on Desktop to simplify users work. For example, placing an Excel shortcut on desktop will easily infer any user how to use it. Furthermore, connection shortcuts are uneditable and therefore provide higher security.
- **Connection Source:** Since connections may origin from various sources (e.g. local / Xcalibur / PNAgent / …etc), for better convenience, it is possible to specify whether to display connections only from specific origin or from all sources.

4.1 "How To" Use My Connection Manager

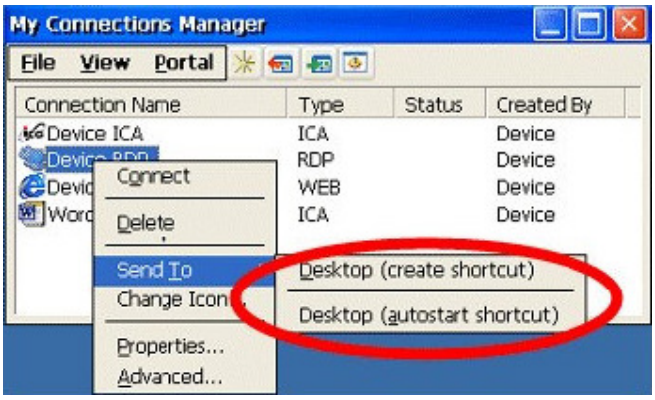
- **Create new connections:** Through the File → New → menu, select the connection type (RDP / ICA / I.E…etc) you wish to create and follow the wizard.



- **Add connection types to the list:** The connection types list is composed of the activated Plug-ins installed on the device. If, for example, the ICA option in not available in the connection type list it suggests that the ICA Plug-in is neither installed nor active. Therefore you need to install the ICA Plug-in, activate it and restart the device.
- **Change connection icon:** In order to change a connection's icon, select it from the connections list, right click, select the 'Change Icon' option and choose an icon from the built-in icons list displayed in the 'Change Icon' window.



- Create a desktop shortcut: In order to create a desktop shortcut select the connections from the connection list, right click it, and from the Send To menu select either the Desktop (create shortcut) or Desktop (auto-start shortcut) option. Auto-start shortcuts have the (A) letter added to the connection icon indicating that these shortcuts launch automatically at the end of the device boot.



- Edit an existing connection: Select the connection from the connection list, right click it and select the Properties option.

- **Delete an existing connection:** Select the connection from the connection list, right click it and select the Delete option. Note that the corresponding desktop shortcut is also deleted.

- **View connections by specific origin:** From the View \ Options menu, select the type of connections to be displayed inside the Connection mode (Xcalibur / PNA / Local / Show All).

- Switch between the 'Connection' and 'Portal' views: From the View menu, select Connections to work in connections mode or Portal to work in the portal mode. A dimmed-out Portal view option indicates this option is not enabled.

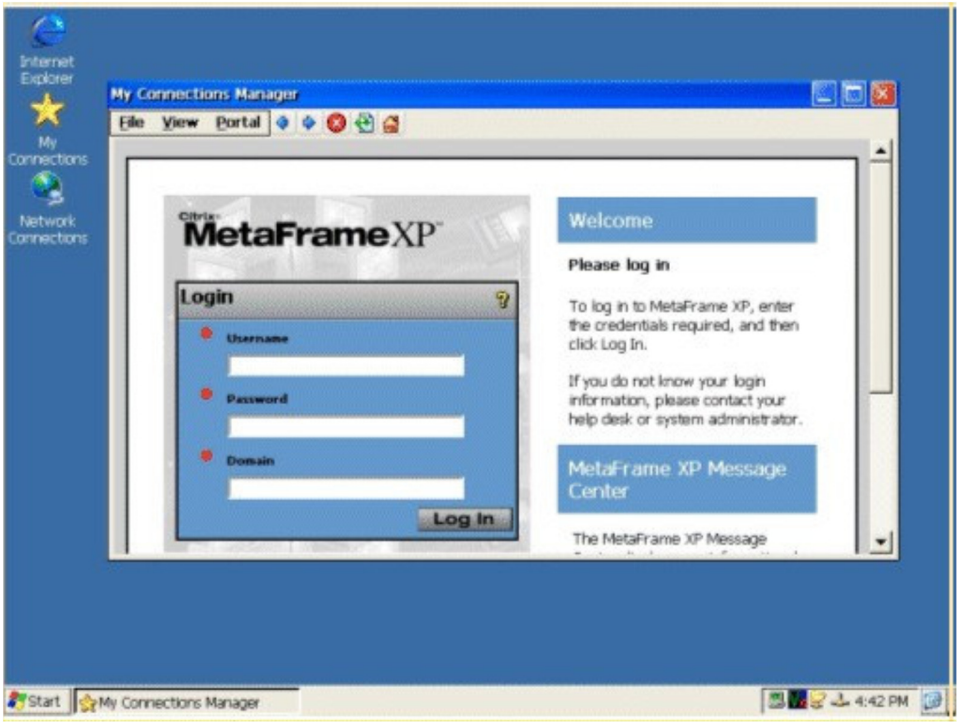
Portal Mode

The Portal mode brings the common working approach of centralized web-based connection management (e.g. Citrix NFUSE) to be realized on the client inside a single limited web browser window.

While in the Portal mode, My Connections Manager runs an Internet Explorer session inside a restricted shell, preventing users from connecting to URLs other than the ones predefined in the Portal mode.

1 Portal Mode Advantages:

- **Pre-specify a URL:** Limit users web access to a pre-specified URL to which My Connections Manager connects automatically. Users are neither able to change the default URL nor specify alternate URL paths since there is no address bar in the Portal window.
- **Highest Web Access Control:** Optionally, prevent users from running web connection other than the 'Portal' connection.
- **Centralized Web-based Connection Management:** Control and centralize connections on a per-user base while providing users a single point of entry to all their applications via the web. Don't bather creating connections locally, simply point 'My Connections Manager – Portal' to the website from which you centralize connections (e.g. Xcalibur Portal / Citrix NFUSE…etc). Once users logon, a connection list is displayed to each user according to his/her credentials.



1.1 How to Use Portal mode

- **Switch between the 'Connection' and 'Portal' views:** From the View menu, select Connections to work in connections mode or Portal to work in the portal mode. A dimmed-out Portal view option indicates this option is not enabled.
- **Enable the 'Portal' mode:** Select the Internet Explorer connection from the My Connection Manager right click and press Advanced tab, select the 'Enable the 'Portal' option in My Connection Manager application' (license dependent) option and specify the default URL for the Portal mode to connect to.
- **Prevent users from running other I.E connections:** Additional security is achieved once selecting the Hide IE connections from connection manager option. This prevents users from running other Internet Explorer connections and therefore limits their web browsing experience only to the 'Portal'* (see Figure 20.2.3).
- **Open as default in 'My Connections Manager':** Makes the 'Portal' mode the default interface of 'My Connection Manager'.
- **Enter multiple URLs via the 'Portal':** In case the web page pointed by the 'Portal' contains URL hyperlinks, those will be opened within the 'Portal' window once selected. This functionality allows users to browse entire web sites following the hyperlinks within them. Administrators are able to control user's browsing by the URL hyperlinks they publish in the 'Portal' web site.

NOTE *In order to completely limit web browsing to the 'Portal' clear the 'Desktop' and 'Application List' shortcut options under the I.E Plug-in properties.*

Chapter 6 Network Manager

The Network Manager tool centralizes network connection management.
Through this interface, users are able to view, run, modify, delete and create new network connections (VPN / Dial-up…etc').

Network Manager Features

- **Link between Network and Application connections:** As part of the network connection settings wizard, one can select an application connection to be launched together with a network connection. This way, for example, a device can be set to launch an ICA connection together with the VPN connection that connects it to a remote network.
- **Connection Shortcuts:** Create connection shortcuts on Desktop or Start menu to simplify users work. For example, placing a Dial-up shortcut on desktop will easily infer any user how to use it. Furthermore, connection shortcuts are un-editable and therefore provide higher security.
- **System Tray indicator:** Dynamically put a remote network indicator item in the System Tray once a connection is active. Active connection details are viewable via this item, indicating the connection name, line details and other TCP/IP information.

How to Use Network Manager

- Create new connections: Go to File → New and follow the wizard.
- Link Network and Application Connections: Go to File → Properties → Login Info, select the Select the connection to launch with this connection option. Than choose the application connection from the list Use the LAN's default gateway while a network connection is active: By default, once a dial-up or virtual private networking connection is made, the remote network default gateway becomes the default for all TCP/IP communication. As result, locations reachable via the original (LAN) default gateway are no longer reachable. Once clearing the 'Use default gateway on remote network' (license dependent) option located under the Network Connection properties \ Connection Properties Tab' the local default gateway remains valid.
- **Allow Auto-Reconnection:** Selecting the Auto-reconnect… option located under the Connection Properties tab specifies whether the connection is redialed if the line is dropped.
- **Create a (desktop / start menu) shortcut:** Select a connection from the connection list, right click it and from the Send To menu select either the Start Menu or Desktop (auto-start shortcut option). Auto Start shortcuts have the (A) letter added to the connection icon indicating these shortcuts launch automatically at the end of the device boot.
- **Edit an existing connection:** Select the connection from the connection list, right click it and select the Properties option.
- **Delete an existing connection:** Select the connection from the connection list, right click it and select the Delete option.
- View active connection information: Double click the network connection system tray item.

This page is left blank intentionally.

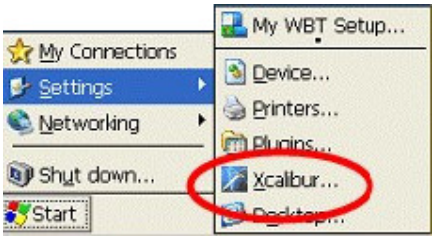
Chapter 7 Xcalibur Dialog – Configuring Management Parameters

The Xcalibur dialog sets different communication parameters associated with Xcalibur Global management software.

Chip PC thin clients remote management process is based on an independent protocol that has a built in support for: SSL, Encryption, Compression, Port number control and more. Different parameters can be changed to enable communication and the discovery of new devices by Xcalibur Global.

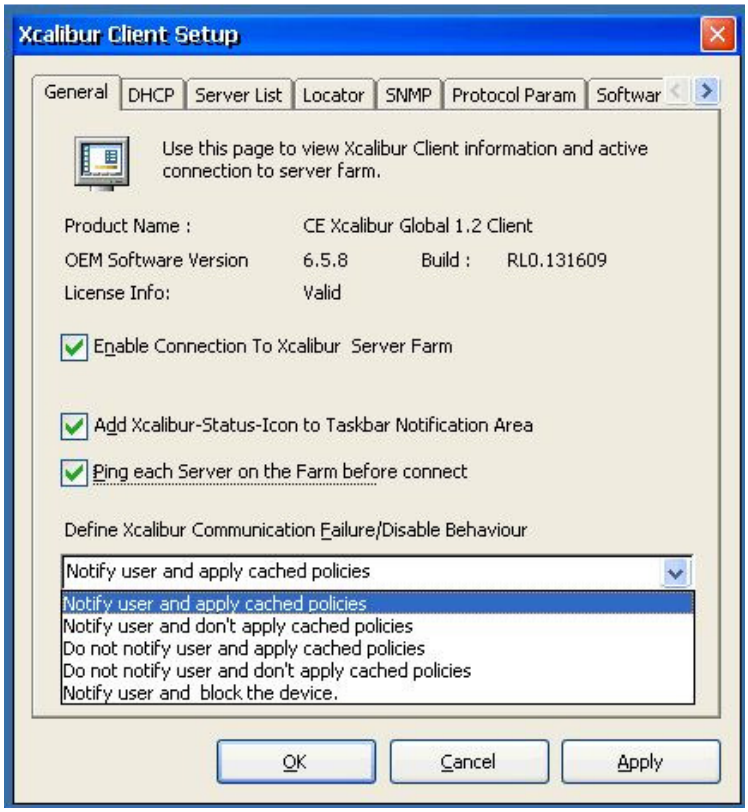
In order to fully understand this chapter it is needed to have at least a basic understanding of Xcalibur Global and its management concepts.

To access the Xcalibur dialog, go to **Start → Settings → Xcalibur**



General Tab

- **Enable Connection to Xcalibur Server Farm:** Mark this checkbox to allow connection to Xcalibur Global.
- **Add Xcalibur Status-Icon to Taskbar Notification Area:** Users can add an icon to their Taskbar to indicating whether they are connected to Xcalibur Global
- **Ping each Server on the Farm before connect:** Test connectivity to Xcalibur Global server before connecting
- **Define Xcalibur Communication Failure/Disable Behavior:** Users can define their device behavior If it failed to create a connection to Xcalibur Global:
  - Notify User and apply cashed policies: Xcalibur Global can control all aspects of device configuration. If the device cannot connect to Xcalibur some of the settings defined by the administrator might be changed. In order to prevent that the user can select this option and apply all the cashed policies on his device.
  - Notify User and Don't apply cashed policies: In some cases the user might want to change the device settings if it is not connected to Xcalibur.
  - Do not notify user and apply cashed policies
  - Do not notify user and do not apply cashed policies

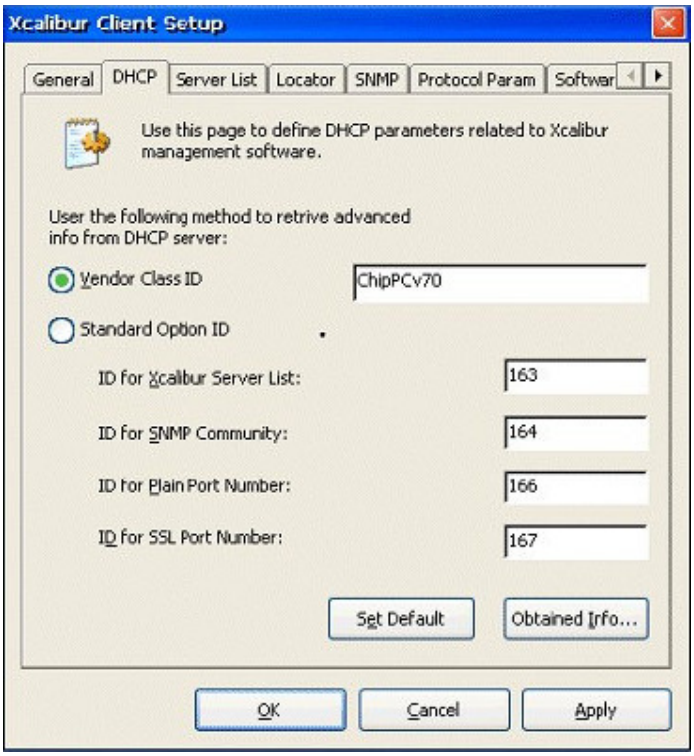

Xcalibur Client Setup
General
DHCP
Server List
Locator
SNMP
Protocol Param
Softwar
Use this page to view Xcalibur Client information and active connection to server farm.
Product Name :
CE Xcalibur Global 1.2 Client
OEM Software Version
6.5.8
Build :
RL0.131609
License Info:
Valid
Enable Connection To Xcalibur Server Farm
Add Xcalibur-Status-Icon to Taskbar Notification Area
Ping each Server on the Farm before connect
Define Xcalibur Communication Failure/Disable Behaviour
Notify user and apply cached policies
Notify user and apply cached policies
Notify user and don't apply cached policies
Do not notify user and apply cached policies
Do not notify user and don't apply cached policies
Notify user and block the device.
OK
Cancel
Apply

DHCP tab

There are several ways for new devices discovery by Xcalibur Global, one of which is using DHCP to pass Xcalibur server information to the device.

In the DHCP tab users can define different parameters relating to DHCP discovery.

- Vendor Class ID: Use Vendor Class
- Standard Option ID: Set the different Option IDs as defined on your DHCP service
- Obtained Info: Press Obtained Info to view information obtained from the DHCP regarding Xcalibur communication



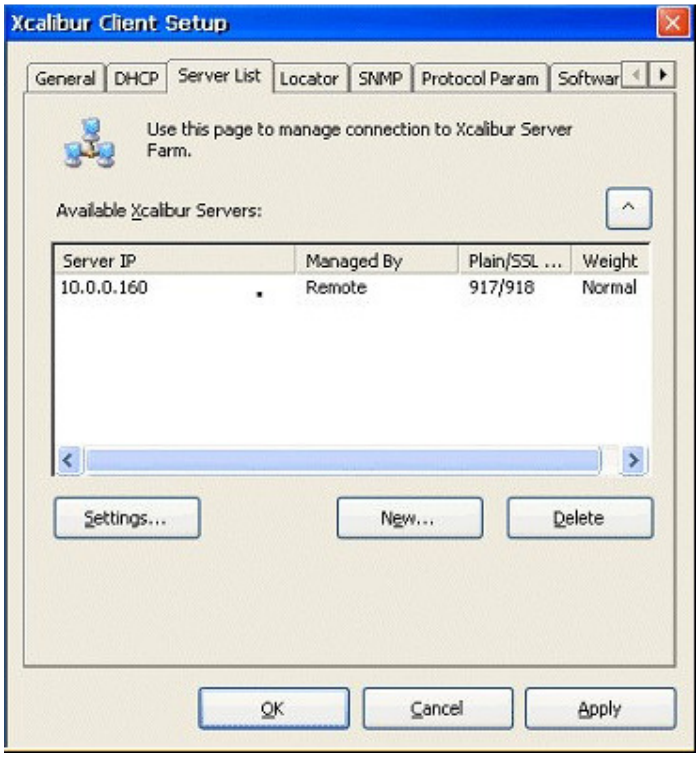
Server List

Devices can be connected to several Xcalibur Front End Servers in order to ensure float tolerance threw Redundancy and Load Balancing.

The list of Xcalibur Front End Servers can be received by the device in several different ways one of which is to define them locally.

Using the Server List tab users are able to define those servers and set their priority in the server list.

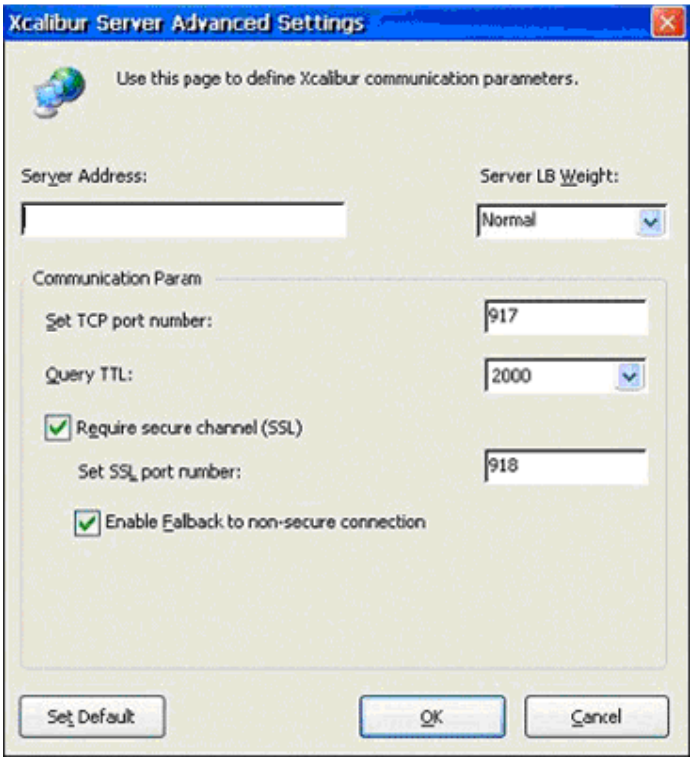
The device will select a server based on its location on the list unless otherwise configured based on the server's priority.



1 Servers Operations

1.1 Add a New Front End Server

- Click **New**
- In the **Server Address** box type the IP address of the Front End Server
- From the **Server LB Weight** select the priority you wish to assign to the server
- Set the **TCP Port Number**
- From the drop down menu Query TTL select the maximal time to wait for a replay from the server before moving to the next server on the list.
- Check **Require Secure Channel** (SSL) in order to enable SSL communication
- Type the port number you wish to use in the Set **SSL port number** check box
- Check **Enable Fallback to non-secure** connection if you wish to enable non-secure connection if a secure one could not be established
- Use the Set Default button to save all current settings as defaults



1.2 Delete a Front End Server

Front End Servers can be deleted by users. In order to delete a FES select the server you wish to delete form the Server List tab and press **Delete**.

1.3 View Server Settings

Select the Front End Server you wish to view and press Settings.

All the server configuration parameters as defined in the Add New Front End Server section will be shown.

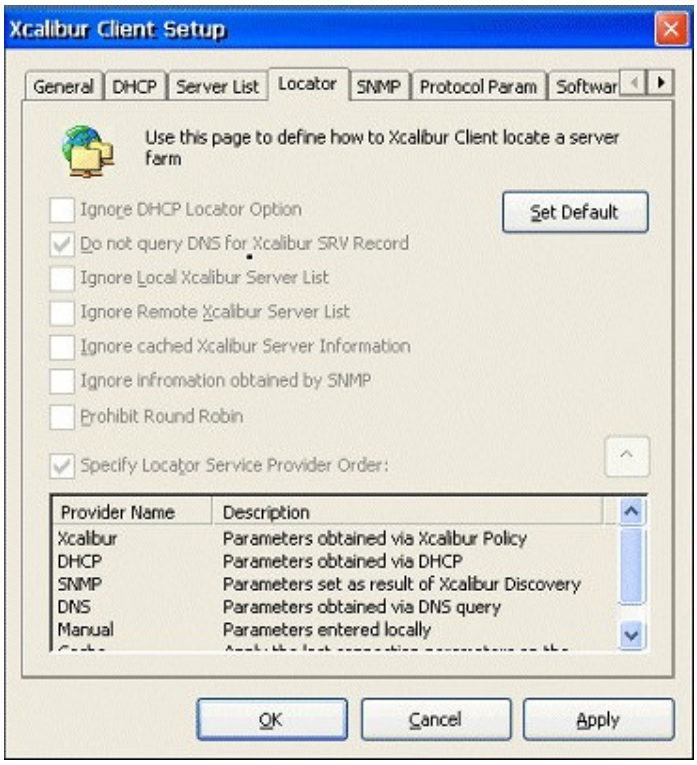
1.4 List Order

Use the arrow on the right to move Front End Servers up on the list of servers' priority.

Locator Tab

Using the Locator tab users can set the different sources of information from which to obtain Xcalibur servers list and the priority of each source.

As mentioned above it is possible to use several Front End Servers and several discovery methods and it is important to set the priority for each server and each source.



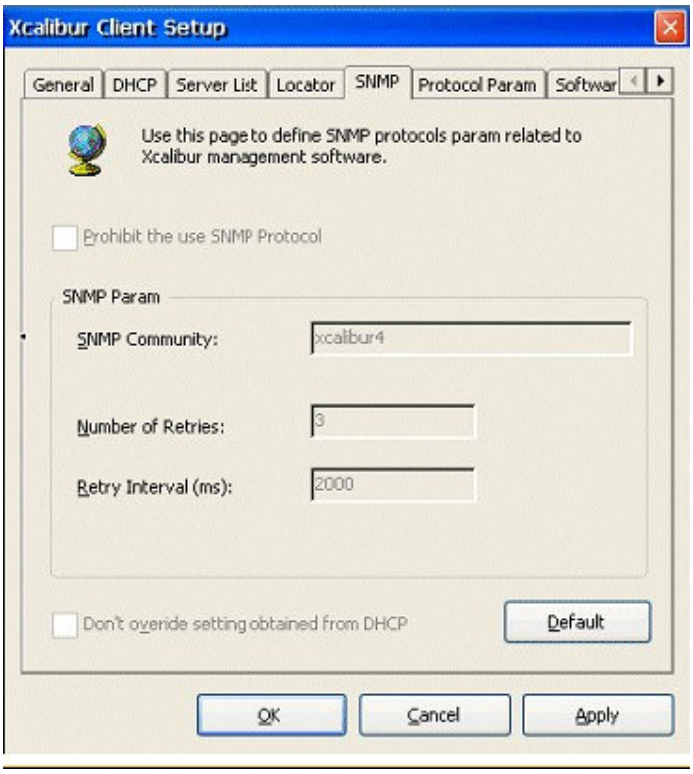
- **Ignore DHCP locator Option:** Unmark this checkbox to allow the use of DHCP as a source for FES list.
- Do Not Query DNS for Xcalibur SRV Record
- **Ignore Local Xcalibur Server List:** Mark this checkbox to ignore the list of servers defined in the Server List tab
- Ignore Remote Xcalibur Server List
- **Ignore cashed Xcalibur Server Information:** Server information is cashed and saved. By marking this checkbox users can choose to ignore the cashed server information.
- **Ignore Information obtained by SNMP:** By marking this checkbox users can ignore server information obtained by SNMP.
- **Prohibit Round Robin:** Once a list of servers is received using the locator service. All devices will connect to the first server on the list. Round Robin randomly assigns devices to all the servers on the list.
- **Specify Locator service Provider Order:** This checkbox enables users to change the priority of the locator service. Check the Specify Locator service Provider Order

checkbox, select the service and use the arrow on the right to change the priority of the locator service.

SNMP Tab

Another way to discover new devices is to use SNMP. Use this tab to configure different SNMP parameters manually.

- **Prohibit the Use of SNMP protocol:** If marked, discovery using SNMP is not enabled
- **SNMP Community:** Define the SNMP community name
- **Number of Retries:** Set the number of discovery attempts the device will take.
- **Retry Interval (ms):** Set the delay between attempts
- **Don't override Settings obtained from DHCP:** Check this check box to give SNMP settings received from DHCP a priority over manual SNMP settings.

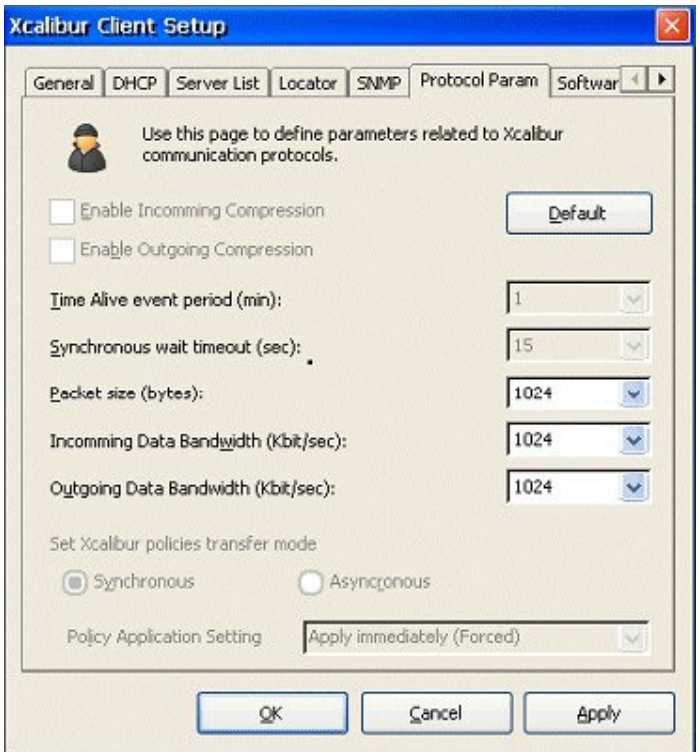


Protocol Parameters

Xcalibur Global uses an independent management protocol. Use the Protocol Parameters tab to configure different parameters relating to the protocol.

- **Enable Incoming/Outgoing Compression:** In order to save bandwidth Xcalibur Independent Management Protocol (XIMP) allows users to compress all incoming and outgoing communication to the Xcalibur server.

- **Time Alive Event (min):** In order to enable accurate reporting in the Xcalibur management console, each device sends a "pulse" to the Xcalibur server. Use this combo box to set the time interval between pulses.
- Synchronous wait timeout
- **Packet Size:** In order to improve bandwidth control users can control the maximal packet size to be sent to Xcalibur server
- **Incoming / Outgoing Data Bandwidth (Kbit/sec):** Select the maximal bandwidth consumption for incoming and outgoing management information to be sent to and from the device.
- Set Xcalibur policies transfer mode
- **Policy application settings:** Use this combo box to decide when will newly applied policy be received by the device:
  - Apply immediately (Forced) – The policy will be applied immediately

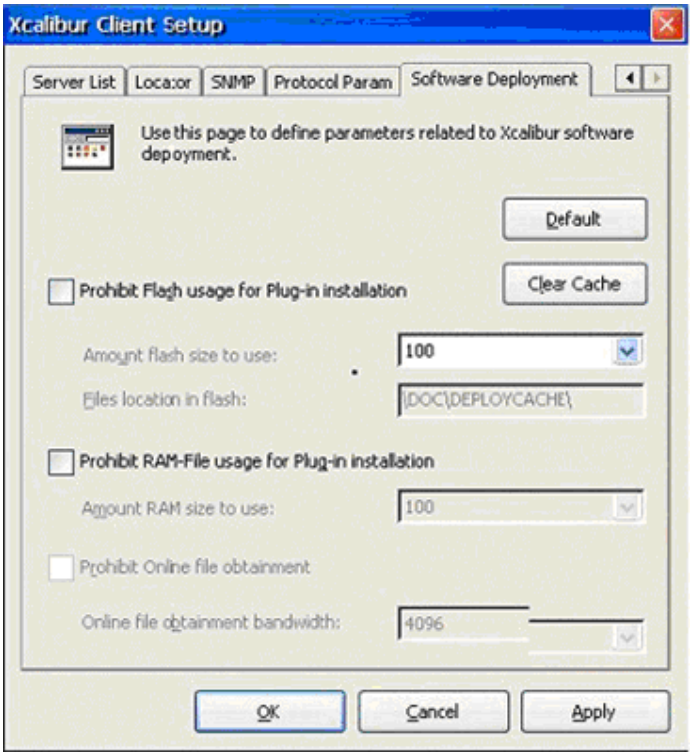


Software Deployment

Plug-ins can be placed by the installation service onto the Flash, Ram File or Online (runs through the network into the RAM-Memory every time). Users can define using the Software Deployment tab where to place the plug-ins.

RAM-File Size - A RAM-File specifies the amount of RAM Memory to be used for Plug-in files storage. Plug-ins installed into RAM-File are retrieved once (during installation) from the network and than run from the RAM-File until the next device reboot. If the software installation is controlled by Xcalibur Policy, once the device is rebooted it will receive the policy again and will have the plug-in on the RAM-File.

- **Prohibit Flash Usage for Plug-in Installation:** This option prevents any Plug-in files from being placed on Flash
- **Amount Flash size to use:** Define how much space can be used for plugin installation.
- **Files Location on Flash:** Configure the location of the plug-in files on the device's Flash.
- **Prohibit RAM-File Usage for Plug-in installation:** This option prevents any Plug-in files from being placed on RAM.
- **Amount RAM size to use:** Set the size of RAM to use for software installation. If the RAM size will be too big it might result in poor performance when trying to use multiple sessions.
- **Prohibit Online File Obtainment:** Plug-ins installed as Online retrieved from the network every time Plug-in files are needed. Online Plug-ins is run from the RAM Memory. In slow bandwidth networks (WANs) you might want to prevent this repeatable network download behavior caused by this mechanism therefore disable it.
- **Online file Obtainment bandwidth:** Set the maximal bandwidth to use for online file obtainment



This page is left blank intentionally.

Chapter 8 Recovery and reset Options

Chip PC thin clients are considered to have excellent Hardware, Firmware and Management therefore recovery process is unusual to occur. However, in order to recover / prevent unexpected failures, several mechanisms are available.

Reset to Default

Chip PC device firmware can be reset to default settings as result of a software or hardware command. A reset to default process results in clearing all device settings and connections, returning the O.S to its initial mode.

Software Reset

Software reset can be initiated via the WBT \ General tab \ Restore \. As default, all manually (and remotely) applied device settings and connections are cleared due to this operation. Additionally, all Plug-in settings are cleared.

1 When to use software reset (examples)?

A software reset may be used when clearing all device settings at once is necessary.

- **Moving devices between environments:** When moving devices between environments, running software reset prior to connecting a device to a new environment is recommended.
- **Device & Plug-in conflict:** When device and/or Plug-in settings seem to conflict, a software reset provides a clean start for device configuration.

Hardware Reset & Safe Mode Operation

A hardware reset can be initiated by running a certain action sequence once pressing the ON/STBY button. As result of this procedure, the device boots into a safe-mode state.

1 What is safe mode?

Safe mode is an intermediate state into which the device boots as a result to a hardware reset. This mode was designed to allow the device to complete its boot in any scenario. While in safe-mode only basic OS components are loaded therefore device settings are unchangeable. Administrators can only perform firmware or hot fix installation during this mode. To exit the safe mode, reboot the device.

As in software reset, all manually (and remotely) applied device settings and connections are cleared due to this operation. Additionally, ALL Plug-in settings are cleared and Plug-in status is set to deactivated*.

2 Complete the following in order to perform a hardware reset:

- Take out (disconnect) the power cord connector from the device socket.

- Plug in the power cord back into its device socket.
- One (1) second after the power is connected the ON/STBY lid shortly blinks (turns on and off), right after this blink, press the ON/STBY button for one (1) second and than release it.
- Once the ON/STBY lid turn red, press the ON/STBY button for one (1) second and than release it.
- Once the ON/STBY lid turns green, press the ON/STBY constantly until the progress bar in the system-splash screen is filled, than release it.

3 How to do Hardware reset On a Jack PC:

- Use a paperclip (or other thin object) to press and hold SW Button (symbol '!' on EFI)
- Press the Reset button on the board (symbol 'RST' on EFI)
- Waite for orange light to turn red and release SW Button
  - For Safe Boot press twice and hold SW Button (green led is blinking) until Safe Mode screen appear
  - For Manual Recovery press and hold SW Button (red light is blinking) until Recovery screen appear

NOTE *This procedure (deliberately) requires timing and accuracy in order to prevent user activation by mistake. Therefore several retries might be necessary before successfully entering the safe-mode.*

4 When to use hardware reset (examples)?

A hardware reset should be used whenever software reset is undoable:

- **Miss configured display:** Miss-configured display settings (e.g. too high screen refresh frequency rate) may result in a clutter of colorful lines or a black screen display. This problem might appear when the monitor does not support the device's screen refresh rate / screen area size defined under the Display Tab. In this scenario, initiating a software reset becomes impossible therefore you can either connect the device to a different monitor or perform a hardware reset.
- **Password Locked WBT:** Incase the WBT Setup environment is inaccessible due to password protection, and the password set is forgotten. A hardware reset clears the password protection making device settings accessible again.

Redundant Boot Options

The following mechanisms are embedded into the device firmware and are launched automatically upon need.

1 Error Correction

In addition to the fact that industry standard DiscOnChip (DOC) with a true file system is used for image storage on the devices. An enhanced error correction mechanism is used for the highest stability of the boot process. The image boot files are highly secured and in some cases doubled for highest tolerance and redundancy.

2 Disk Surface Check

During boot a disk surface scan process verifies every block in the file system. This process is designed to prevent the usage of a bad block which may interfere with the O.S operation.

Once an error is discovered, the scan disk process automatically marks the block as 'Bad Block' and attempts to replaces it with a new block obtained from the 'Block Reserve' area which contains approximately 1Mb of free blocks. 'Bad Blocks' are mapped and therefore will never be used again.

Incase a block replacement failure is recognized as a corrupted file system, the device automatically loads a primal firmware image into the memory and initiates a remote recovery mode also known as PXE mode.

PXE Mode

PXE boot mode is considered to be a poor remote management solution for image updates.

Chip PC has developed a variety of advanced update, manage and recovery mechanisms making the PXE use unnecessary and much less functional compared to these alternatives.

However, in order to provide the highest flexibility and reliability, PXE Boot is supported by the EX family devices. PXE boot mode is launched automatically incase of a fatal image crash, allowing the device to obtain a new image from a PXE Server.

1 What is PXE Mode?

Pre-Boot Execution Environment allows a device to boot from a server on a network prior to booting the operating system on the local Disk on Chip (DOC).

2 How Does PXE Recovery Work?

- **PXE boot mode** is launched automatically incase of a fatal image crash, allowing the device to obtain a new image from a PXE Server.
- **PXE server connection:** The PXE server watches for DHCP Discovery requests that include a special tag identifying the client as a PXE client. If the discovery request includes the tag, the PXE server replies to the client with configuration information, including the name of a boot image file. The boot image file is transferred to the client, and this file is then used to boot the client.

This page is left blank intentionally.

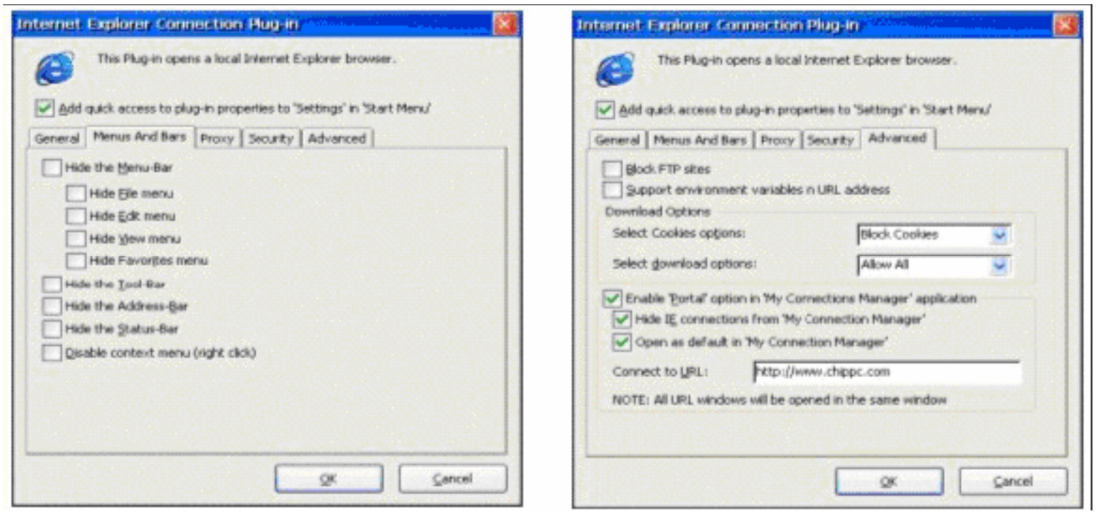
Chapter 9 Image 7.0.x Advanced Plug-ins Configuration

New Internet Explorer Options by Chip PC

Microsoft Internet Explorer 6.x (for CE.NET v4.2) is installable on firmware version 7.0.X devices as a Plug-in. Due to the increasing demand for customization, security and control of user environment this enhanced Internet Explorer (I.E) version includes additional features to answer field demands.

New Features in IE

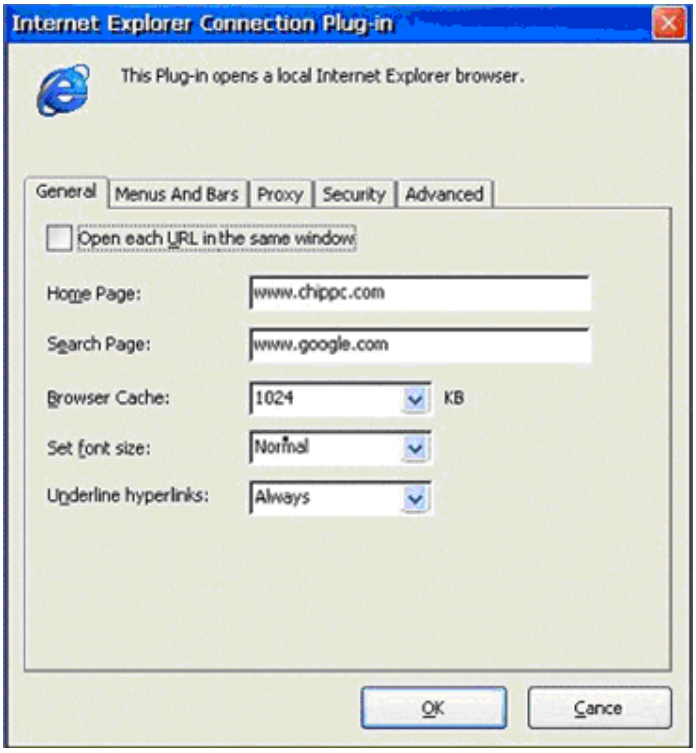
- **Fully customizable shell:** In addition to all standard I.E settings such as Home Page, Proxy, Font size etcetera, administrators now have full control of the Internet Explorer shell. With the option to hide menus and bars you can limit users' web experience to meet your demands.
- **Limit FTP / Cookies and other download options:** Users downloading unfamiliar files from the internet will always be a hazard to IT environments. Therefore in high security scenarios, some would like to prohibit all web downloads while others need to compartmentalize safe downloads from potentially dangerous ones. Enhanced download control options let you adjust I.E security to any security level
- **Platform Identifier selection options:** Once connecting to any website via a web browser, the browser identifies itself and its hosting operating system to the website. This information can be used by the website to filter content and security settings on per client web browser and O.S bases. Internet Explorer Plug-in version 6.0.04 allows changing the default (Windows CE) platform identification.
- **Secured 'Portal' Viewer:** Within two mouse clicks apply the most strict shell security options by limiting all web access through My Connections Manager \ Portal view.



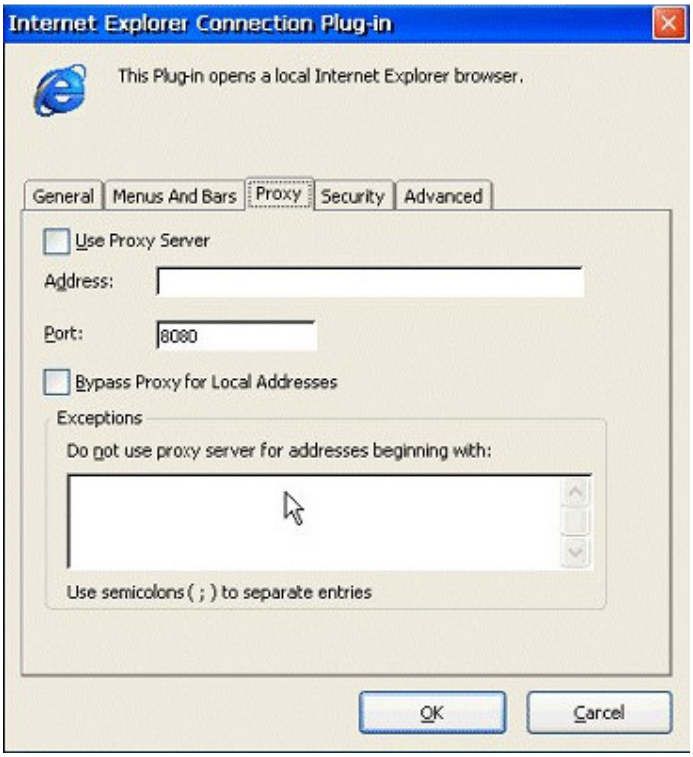
How To Customize the IE plug-in

- **Customize I.E defaults:** Through the general tab of the Internet Explorer Connection Plug-in you can define different parameters regarding IE defaults: Home Page, Search Page, Cache size, Font Size and more.
- **Customize I.E shell:** Through the Internet Explorer Plug-in \ Configuration \ Menus and Bars dialog you can decide which I.E menus to hide while others remain available for use.
- **Prevent access to FTP sites:** By selecting the Block FTP sites option under the Advanced dialog URL's pointing to FTP sites become inaccessible.
- **Control Cookies:** Cookies are small text files used for local information storage by some websites. Through the 'Select Cookies options' combo box you can choose whether to allow or prevent cookies from being saved locally. Options other than the 'Block Cookies' specify the amount of local storage space to be allocated for cookies. Note that if you do not allow cookies at all, users may not be able to view some web sites or take advantage of customization features (such as local news and weather, or stock quotes).
- **Sort downloads:** Download options divide into three alternatives; Allow All which lets any file type to be downloaded via the web. Prohibit All which prevents all file downloads, and Allow Connection Only which limits downloads to application connection files only. Use this option when file downloads are forbidden but still users need to access Citrix NFUSE / Xcalibur Portal for running applications. The Allow Connection Only option allows application connection file downloads (e.g. *.ICA / *.RDP / *.per…etc) while preventing all others.
- **Enable the 'Portal' mode:** Through the Internet Explorer \ Configuration \ Advanced dialog, select the Enable the 'Portal' option in 'My Connection Manager' application (license dependent) option and specify the default URL for the 'Portal' mode to connect to.
- **Use environment variables in URL address:** Environment variables are unique identifiers related to client devices. For example, computer name, MAC, IP….etc. When support for environment variables in URL addresses is enabled via the Internet Explorer (properties) \ Advanced Tab, administrators can redirect client devices to specific URLs based on client's environment variables.
  - Example:
    If you're a web master of www.chippc.com and you want to automatically redirect specific devices (e.g. device1 and device2) that connect to this site to specific web pages. You can create the following link: http://www.chippc.com/%computername% which points to multiple html pages -> device1.html / device2.html….etc. By supporting environment variables, 'device1' will be redirected to http://www.chippc.com/device1.html, and 'device2' will be redirected to http://www.chippc.com/device2.html.
- **Configure platform identifier options:** Through the Internet Explorer (properties) \ Security Tab, one can choose whether the device be identified as a Windows CE device (default) or as another O.S version. In order to change the O.S identification select the 'Identify My Station as:' option and type the O.S version you wish to be identified as. (For Example: In order to be identified as a Windows NT 4.0 client type: Windows NT 4.0).

- **Internet Explorer Proxy Sever:** Through the Proxy tab you can define and configure the use of proxy server to accelerate the use the Internet Explorer.



- **Security:** Through the Security tab you can define different settings regarding the IE security settings.



NOTE *Modifying the platform identifier settings may cause web browser instability and website mismatches therefore should be used by advanced users only. The platform identifier option is supported by Internet Explorer Plug-in version 6.0.04.*

New RDP Features Introduced by Chip PC

Microsoft RDP client version 5.x is installable as a Plug-in on firmware 7.0.X devices.

Once installed, it is operational in two working modes, Native and Advanced.

- **Native** operation mode runs the original, unmodified, Microsoft RDP client application accessible only through the 'Remote Desktop Connections' desktop shortcut.
- **Advanced** operation mode runs an enhanced RDP client including new features built to improve users' and administrators' experience of RDP protocol. All connections built by the 'My Connections Manager' use the advanced RDP version.

New Features:

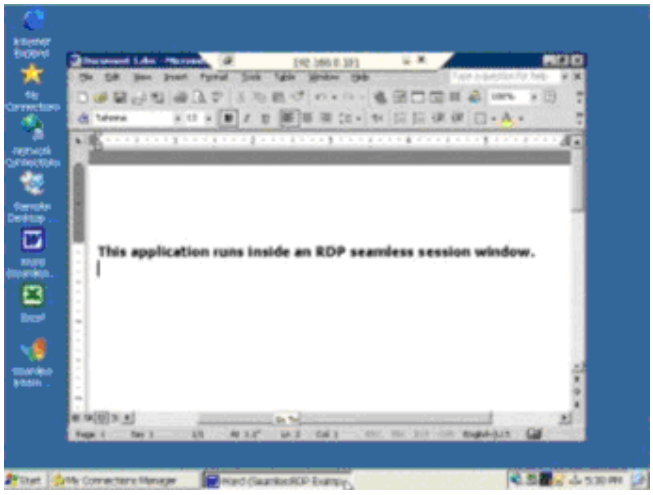
- RDP Seamless Window
- Pass-through authentication
- RDP Load Balanced Connections
- RDP WAN Optimization

1 RDP Seamless Window

A seamless application session is displayed on the client device in such a manner so as to mimic or match that of an application that is launched locally. For example: When launching Internet Explorer seamlessly from a Microsoft Terminal server and also locally, both windows basically looks and behaves the same.

RDP Seamless Window option allows running an RDP session in a window size equal or smaller than the device screen area, where the 'Session Window Name' and the 'Session Window Icon' reflect the application launched (within the session). While minimized, the 'Session Window Name' and the 'Session Window Icon' are displayed in the taskbar.

With **RDP Seamless Window** sessions users find navigating between multiple applications easier while administrators benefit from better server performance, higher security and lower costs.

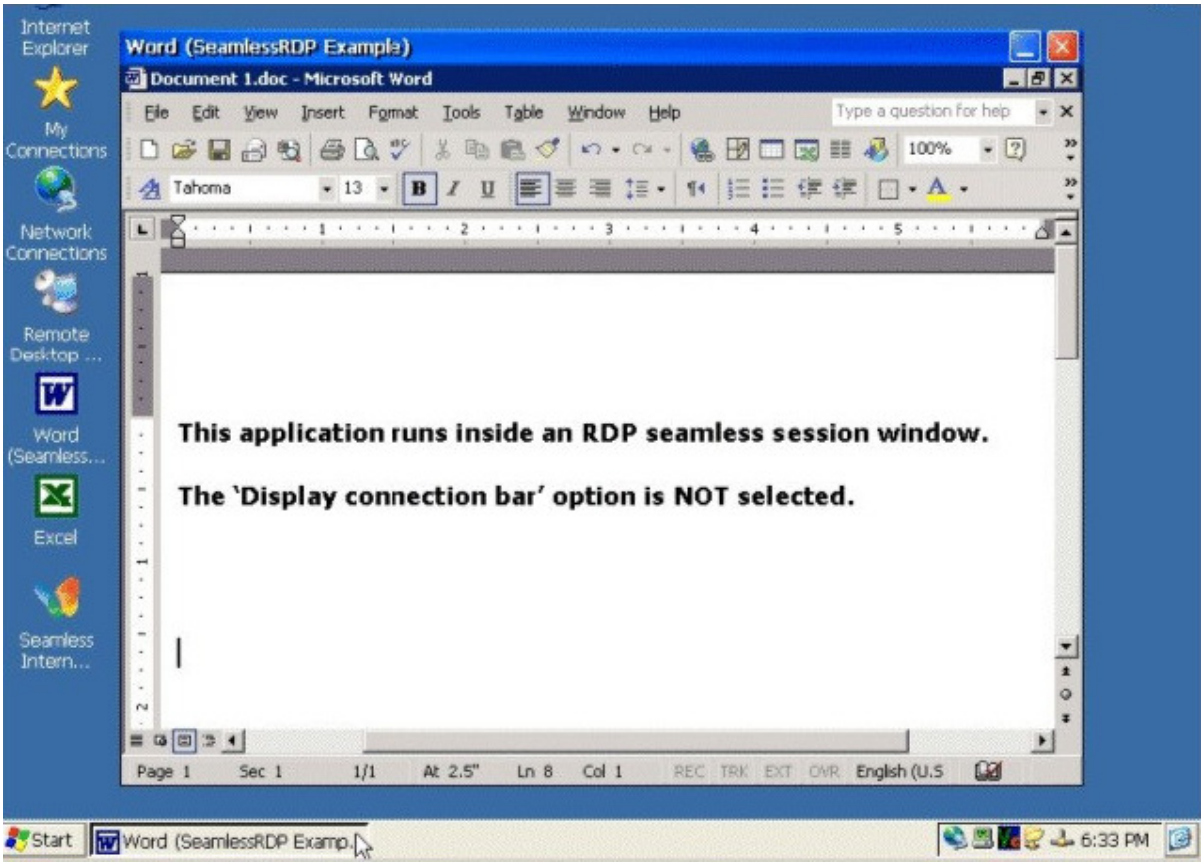


1.1 How to Configure RDP Connection:

- **Configure RDP Seamless Window Session:** Either full desktop or specific application can be run within an RDP seamless window session. Configuring an RDP connection to run seamlessly is done via the Experience tab found under the connection properties.
- **Set the session window size:** State the size of the remote desktop session window by specifying the window width and height values.
- **Set the session frame:** The session frame defines the appearance of the border line between the session window and the local device. Enabling the 'Display connection bar' option results in a connection-bar displayed at the top of the session window. Clearing this option, results in a Window-Title frame presenting the connection name on top of the session window.
- **Open connection in Full Screen:** Once selected the connection launches in full screen mode. Even if the session window size is set to be smaller than the screen area, once this option is on, the session frame covers all the screen area. Therefore, clear this option in order to work seamlessly. Selecting the Fit session view port to

window option allows auto-adjustment of the session window to the local device screen area settings.

NOTE *Set the Connection-icon by using the Change Icon… option via the My Connection Manager as previously explained.*

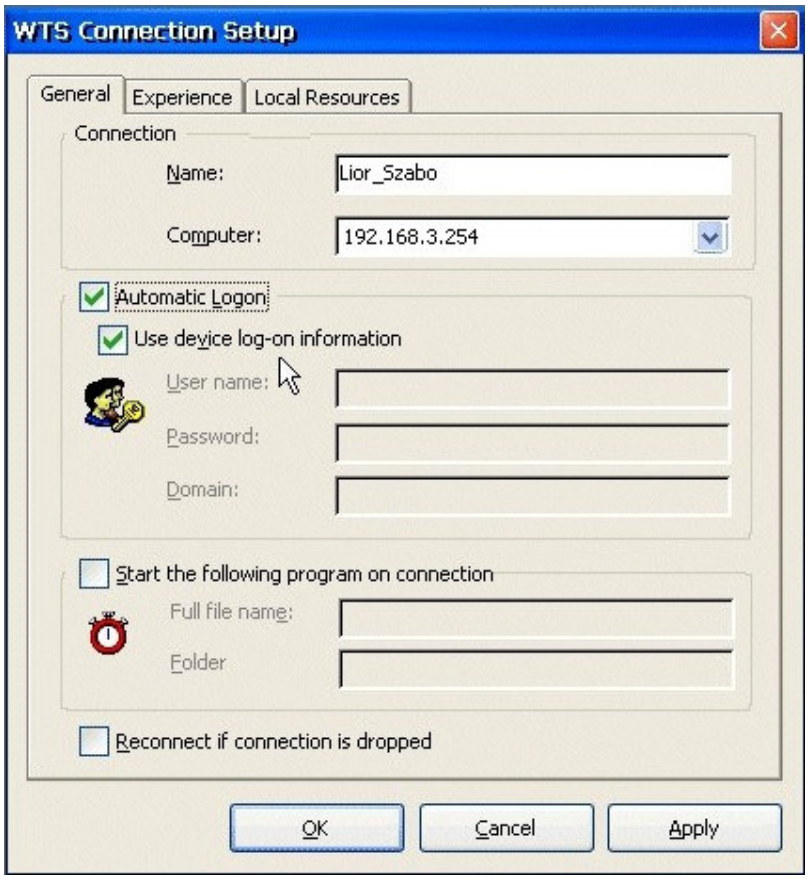

Internet Explorer
My Connections
Network Connections
Remote Desktop ...
Word (Seamless...
Excel
Seamless Intern...
Word (SeamlessRDP Examples)
Document 1.doc - Microsoft Word
File Edit View Insert Format Tools Table Window Help
Type a question for help
Tahoma
13
100%
This application runs inside an RDP seamless session window.
The 'Display connection bar' option is NOT selected.
Page 1 Sec 1 1/1 At 2.5" Ln 8 Col 1 REC TRK EXT OVR English (U.S
Start
Word (SeamlessRDP Examp...
6:33 PM

2 Pass-through Authentication

Pass-through authentication: Thanks to the built-in authentication capabilities embedded into image version 6.x, Chip PC devices are currently the only WinCE clients capable of supporting single sign-on within RDP sessions. Logged-on user credentials provided during device logon may be mapped into RDP sessions while connecting to the server. Therefore users do not have to supply their logon credentials again.

2.1 How To Guide:

Enable Pass-through authentication in RDP: Configuring an RDP connection to use the logged-on user credentials is done via the 'General Tab' found under the connection properties by selecting the 'Use device log-on information' option.



3 RDP Load Balanced Connections

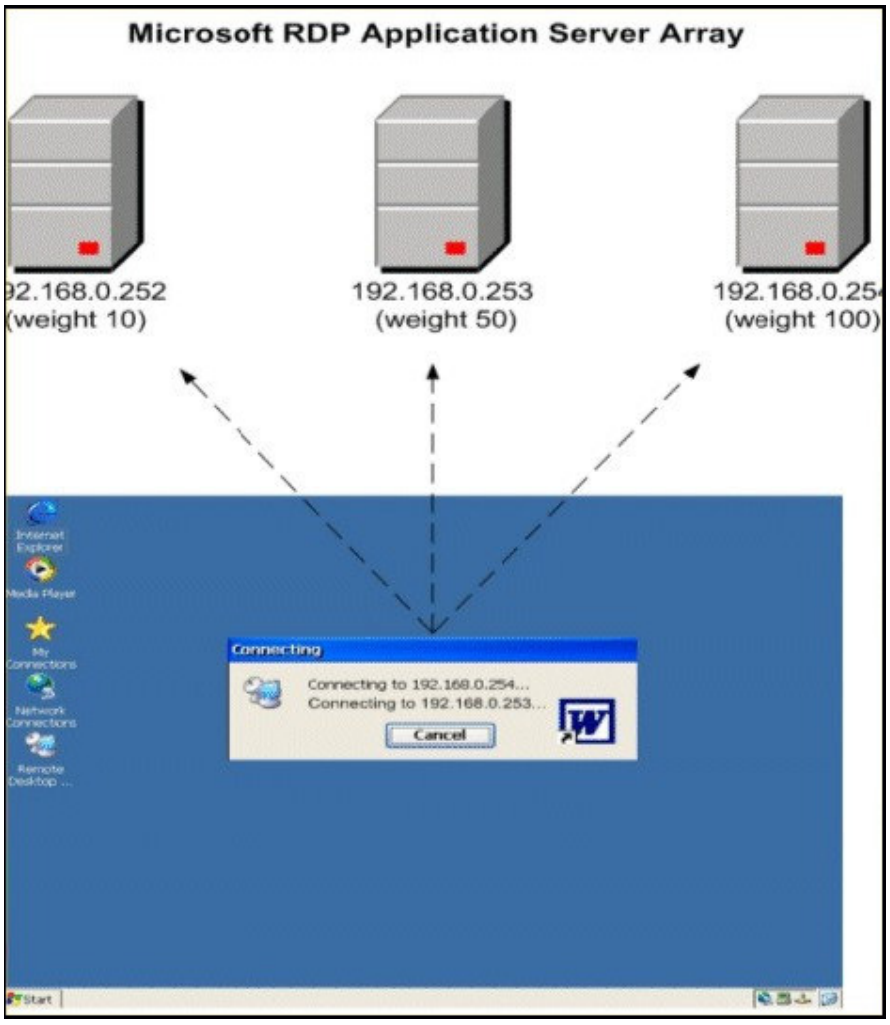
RDP Load Balanced connections balance session loads across RDP servers based on a round robin mechanism by grouping multiple servers under one logical connection name.

In an RDP Load Balanced (RDP-LB) connection setting, one can specify up to ten server names or IPs to which the connection points to. A weight value assigned to each server defines the priority preference towards that specific host.

Once launched, an RDP-LB connection dynamically connects to any group member whilst server's weight calculation is taken under account. Thus divide server loads between multiple servers allowing you to optimize server resources throughout a server array.

Redundancy is also achieved by means of connecting users to multiple servers which all provide an identical work environment. Therefore servers that go unpredictably down do not influence users work as long as other group members are connectable.

The simplicity within the RDP Load Balanced connections mechanism makes it a firm, efficient and cost saving way of load balancing implementation. Especially since it is a pure client-side solution, no server side settings or any software agent installation is needed and no "Middle-Server" is required for session load balancing.

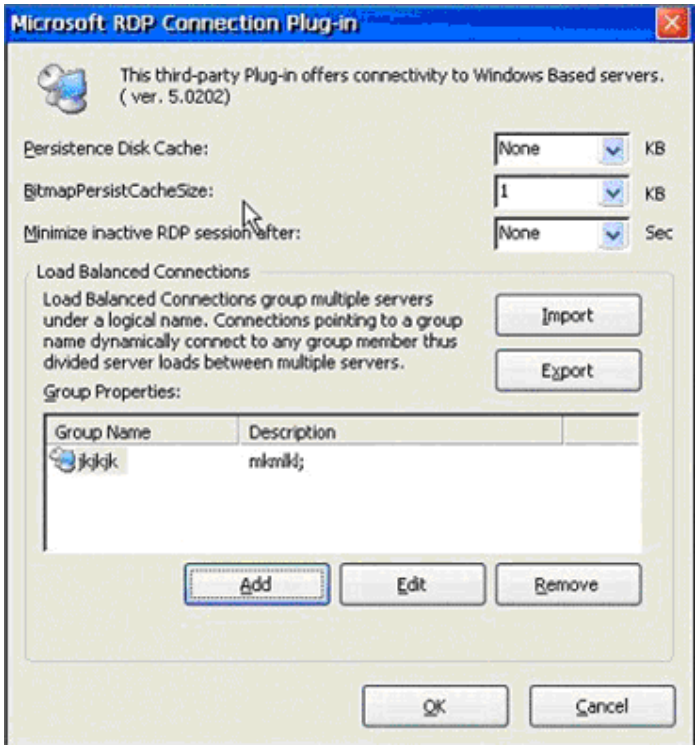


3.1 "How To" Guide:

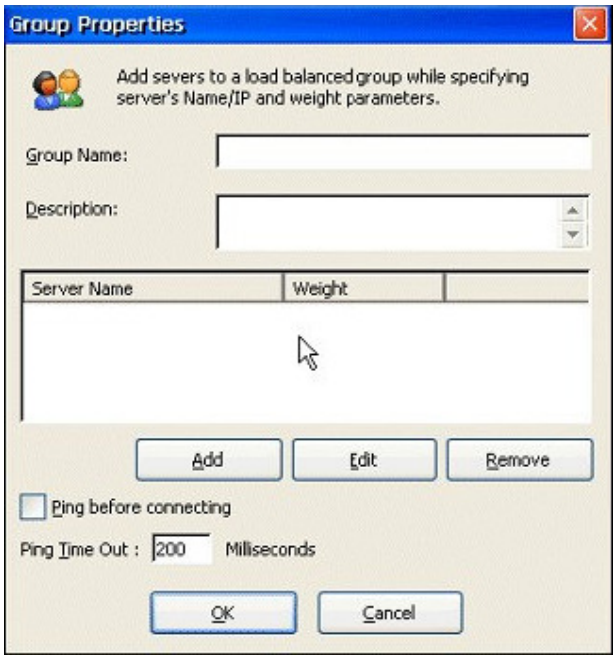
Create RDP Load Balanced Connections Group: To create RDP Load Balanced Connections:

1 Select the RDP plug-in from the Plug-in tab of the WBT dialog

2 Click **Configure**



3 Click **Add**

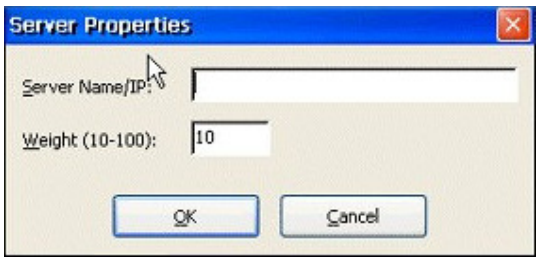


4 Type Group Name, Description

5 Mark **Ping before connecting** checkbox if you want to ping each server before attempting to connect to it

6 Define the ping timeout in the **Ping Time Out** textbox

7 Click **Add**



8 Type the **server name/IP** in the Sever Name/IP text box

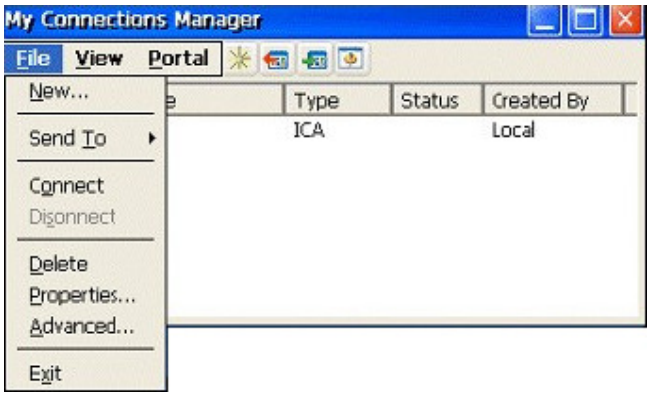
9 Enter the server's weight in the **Weight** text box.

10 Click **OK** to close all dialogs and restart

11 Assign a Load Balanced Server Group to an RDP connection

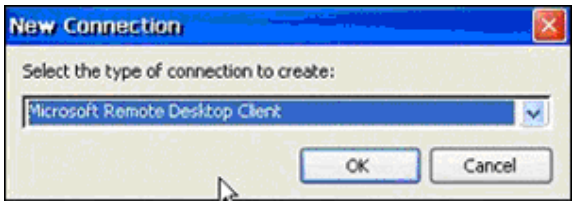
12 Open the My Connections Manager by clicking on the My Connection icon on your desktop.

13 From the File menu select **New**



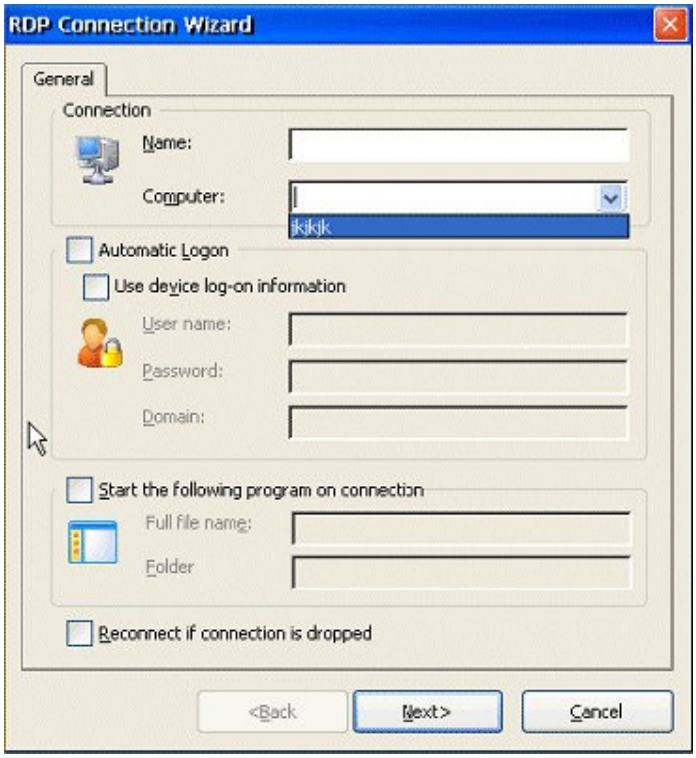
14 From the combo box select Microsoft Remote Desktop Client

15 Click **OK**



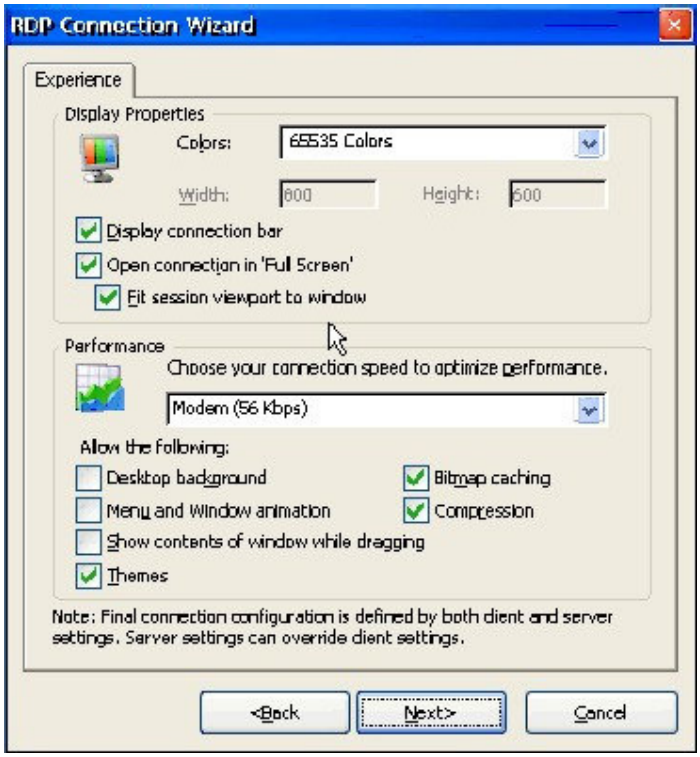
16 Type the connection name in the Name text box

17 Type the IP address of the server or the name of the **Load Balanced Server Group**

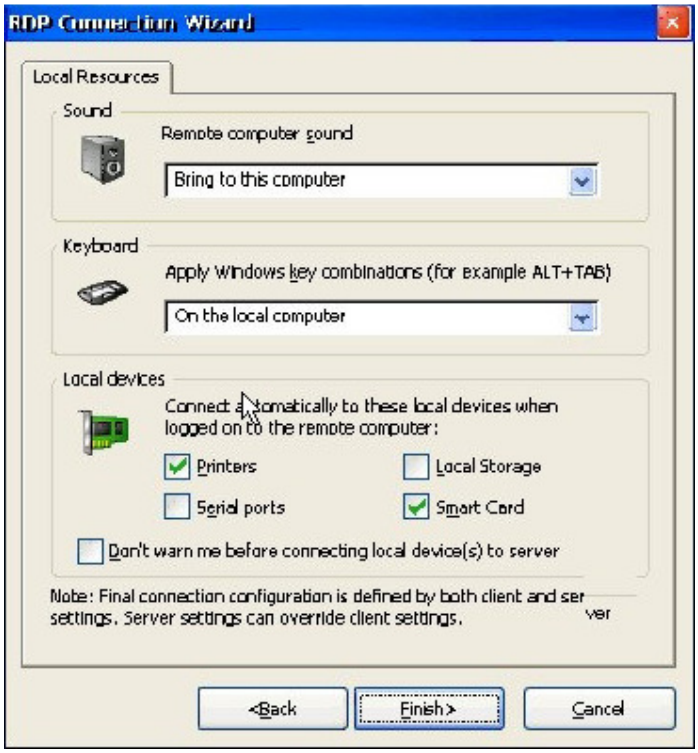


18 Click **Next**

19 Use the dialogs to configure all parameters relating to the RDP connection



20 Click **Next**


RDP Connection Wizard
Local Resources
Sound
Remote computer sound
Bring to this computer
Keyboard
Apply Windows key combinations (for example ALT+TAB)
On the local computer
Local devices
Connect automatically to these local devices when logged on to the remote computer:
Printers
Local Storage
Serial ports
Smart Card
Don't warn me before connecting local device(s) to server
Note: Final connection configuration is defined by both client and server settings. Server settings can override client settings.
<Back
Finish>
Cancel

21 Click **Finished**

4 RDP WAN Optimization

In order to optimize RDP performance towards WANs the following functionalities were added to the RDP client running on Chip PC image 7.0.x devices. These options allow bandwidth saving and better session performance while establishing RDP sessions in low bandwidth environments.

5 Minimized RDP Bandwidth

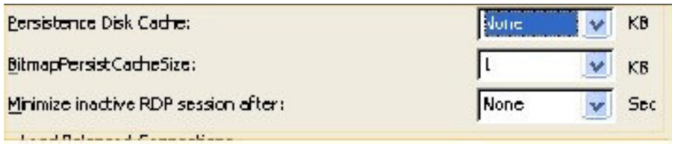
The Minimized RDP Bandwidth built-in functionality automatically reduces the amount of data sent via an RDP session once the session window is minimized to the taskbar. The bandwidth consumption of a minimized-session (an RDP session that is minimized to the taskbar) gets closer to zero transferring only 'keep alive' data between the client and the server.

Thanks to the **Minimized RDP Bandwidth** functionality, scenarios where a user running multiple RDP sessions over a low bandwidth connection while consuming bandwidth for only a single session (the one with the active window) now become possible.

This functionality is built-in to the RDP Client running on image v7.0.x devices. Session windows can be either minimized manually (by the user) or automatically after a specific idle time. The Minimize inactive RDP session after ### seconds combo box located under the RDP Plug-in / Configure allows specifying the amount of idle time after which idle session windows are automatically minimized to the taskbar. In addition, once the local screen saver is in action all RDP sessions are minimized in order to save bandwidth.

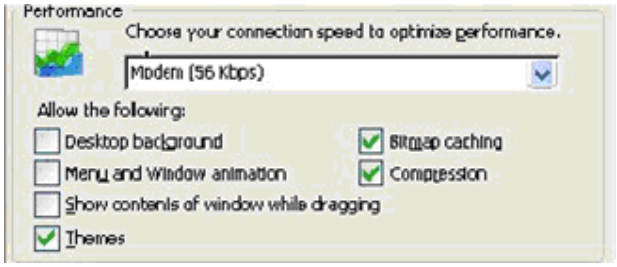
6 Disk & RAM Caching

Disk & RAM caching allow preserving local disk cache and RAM cache for better RDP performance. These settings can be found under the RDP Plug-in / Configure dialog. Use the Persistence Disk Cache to control the cache size.



7 Bandwidth Compression

Bandwidth compression is a built-in functionality available in RDP protocol. Selecting the Compression flag located under any My Connection Manager → RDP Connection → Properties → Experience Tab → Performance Section, enables this option. Compressed sessions consume up to 30% less bandwidth than un-compressed sessions in certain session peaks thus allow preserving precious network bandwidth in low-bandwidth environments.



New WinVNC Options Introduced by Chip PC

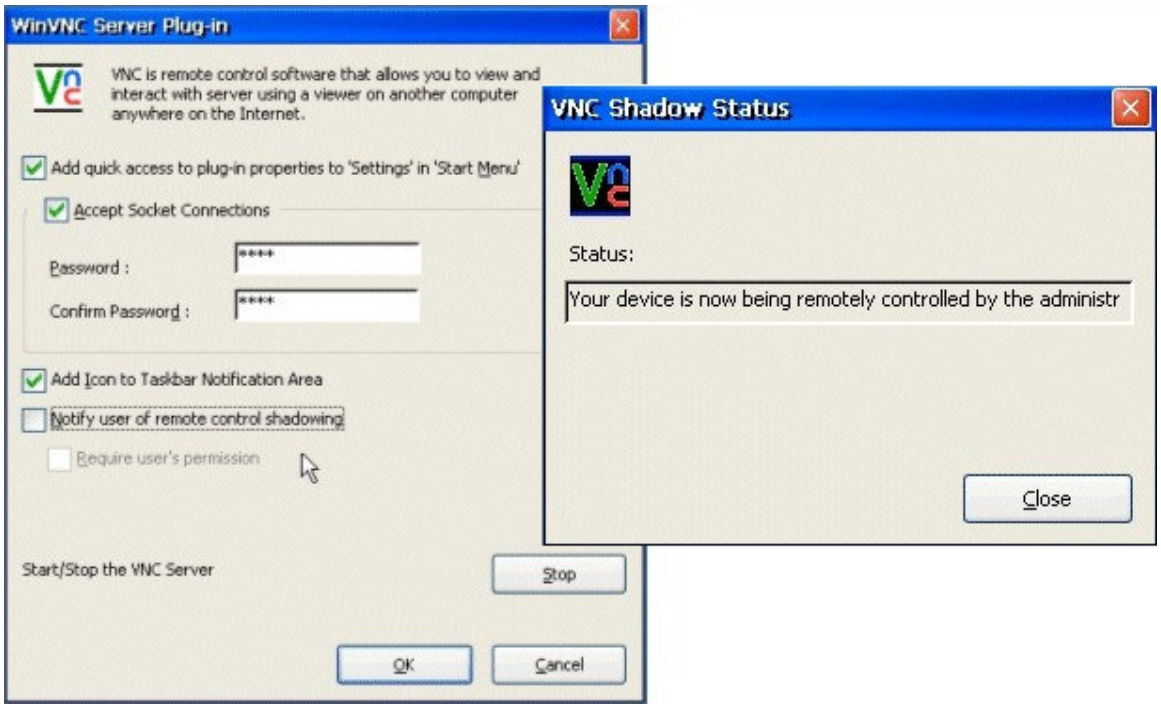
WinVNC Server is installable as a Plug-in on firmware 7.0.x devices. VNC is a remote control software which allows you to view and interact with a device (the "server"), using a simple program (the "viewer") on a computer anywhere on the network.

1 Privacy Options

As default, prior to shadowing a device via VNC no warning or request is presented to the user who is working on the device. Thus may interfere with the user's privacy and confidentiality.

The **Notify user of remote control shadowing** option found under the WinVNC Server Plug-in Configure dialog, creates an on screen event notifying the user his/her device is being remotely controlled. Additionally, the VNC system tray icon color is changed as long as the remote control operation continues.

Higher level of privacy may be given to users by selecting the require user's permission option. Making a remote control operation is dependent on user's approval.


WinVNC Server Plug-in
VNC is remote control software that allows you to view and interact with server using a viewer on another computer anywhere on the Internet.
Add quick access to plug-in properties to 'Settings' in 'Start Menu'
Accept Socket Connections
Password :
Confirm Password :
Add Icon to Taskbar Notification Area
Notify user of remote control shadowing
Require user's permission
Start/Stop the VNC Server
Stop
OK
Cancel
VNC Shadow Status
Status:
Your device is now being remotely controlled by the administr
Close

NOTE *Privacy VNC Options are license dependent.*

Key Citrix ICA 11.100 Options Supported by Chip PC

Not only that image version 7.0.X supports the standard ICA 11.1x client features such as PNAgent, Smartcard etc. Chip PC supports various additional capabilities to enhance the ICA experience and make it as close as possible to the full Win32 ICA client.

1 Program Neighborhood Agent

Citrix Program Neighborhood Agent (PNAgent) allows users to connect without using a Web Browser to a server running the Citrix Web Interface and access all published applications in the server farm.

You do not have to manually configure a connection to each application as you do locally with the My Connection Manager since the Program Neighborhood Agent configuration settings are centrally stored on the server in a file called Config.xml.

After successfully authenticating user credentials, PNAgent client devices read connection configuration data from the server whilst presenting those as a list of applications within the My Connection Manager.

Each user's application list differs according to his/her credentials used for the PNAgent authentication.

2 New WinCE PNAgent client options supported by Chip

2.1 PC:

- **Pass-through authentication:** Thanks to the built-in authentication capabilities embedded into image version 7.0.X, Chip PC devices are currently the only WinCE clients capable of supporting single sign-on within ICA & PNAgent sessions. Logged-on user credentials provided during device logon may be used by the PNAgent while connecting to the server. Therefore users do not have to supply their logon credentials again not even during connections launch.
- **Application shortcut placement:** While publishing an application on a Citrix server, administrators can specify an Application shortcut to be created within the desktop and/or 'Start' menu of a Win32 ICA client. Chip PC devices support application shortcuts creation in either 'Start Menu' or Desktop as defined by the administrator. This functionality of Desktop and 'Start Menu' application shortcut placement allows greater flexibility and control of user's display for the benefit of user friendliness and remote connection administration.
- **Control PNAgent process duration:** The process of connection obtainment via PNAgent occurs during the last stages of the device boot / user logon. As part of this process connection information is passed between the Web Interface server and the client device. Since this procedure is based upon network speed (which can be slow in some cases) original PNAgent process duration might not be enough for the operation to complete. Specifying PNAgent process duration which is now possible allows better adjustment to various networking scenarios.
- **Auto-start PNAgent Connections:** Connections retrieved via PNAgent can be set to be launched automatically (auto-start). This added functionality allows administrators to

configure a published application to be started immediately once its connection gets to the client device.

- **Seamless Windows:** Citrix Program Neighborhood Agent (PNAgent) allows users to connect without using a Web browser to a server running the Citrix Web Interface and access all published applications in the server farm. There is no need to manually configure a connection to each application as done locally with Connection Manager, since the Program Neighborhood Agent configuration settings are centrally stored on the server in a file called Config.xml. After successfully authenticating user credentials, PNAgent client devices read the connection configuration data from the server whilst presenting those as a list of applications within the Connection Manager. Each user's application list differs according to the users credentials used for the PNAgent authentication.

2.2 Other Features in ICA 11.1 Connection settings

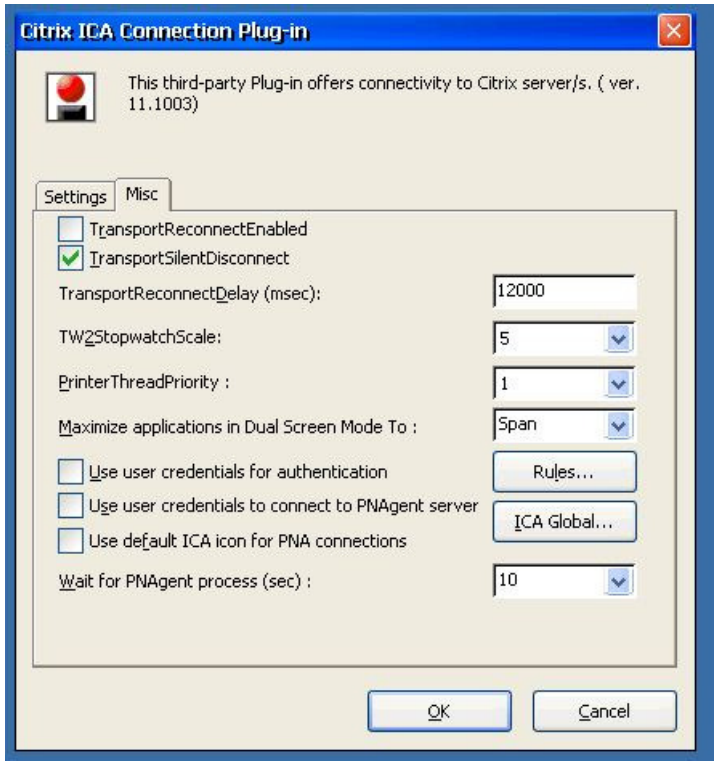
- **Local ICA Connection Icons:** By default, all WinCE ICA client connections can only be assigned with the default ICA icon. Due to the built-in changeable icon support in image 7.0.X, ICA connection icons can be changed to better reflect the application they correspond to. In addition, the connection icon is displayed in the Taskbar while the session is launched.
- **Smartcard and Local Storage Mapping:** Both smartcard and local storage mapping can be generally controlled via the ICA Plug-in properties. This way, administrators can centrally prohibit or allow these object mappings.
- **Disc Caching for Improved Performance:** Disk caching stores commonly used graphical objects such as bitmaps in a local cache on the client's disk on chip (DOC) space. If the connection is bandwidth-limited, using disk caching increases performance.
- **Apply Windows Key Combination:** Once installing HotFix 2 and ICA Plug-in version 7.23.24824.1 one can decide whether to apply Windows key combinations (e.g. ALT+TAB) locally or remotely.
- **Support for Passing Parameters to Citrix MetaFrame Applications:** Many applications may require startup parameters, to be used for various purposes, such as user credentials, underlying database specifications, etc. ICA Plug-in supports passing parameters written under the 'LongCommandLine' field as long as these are written in a single line.

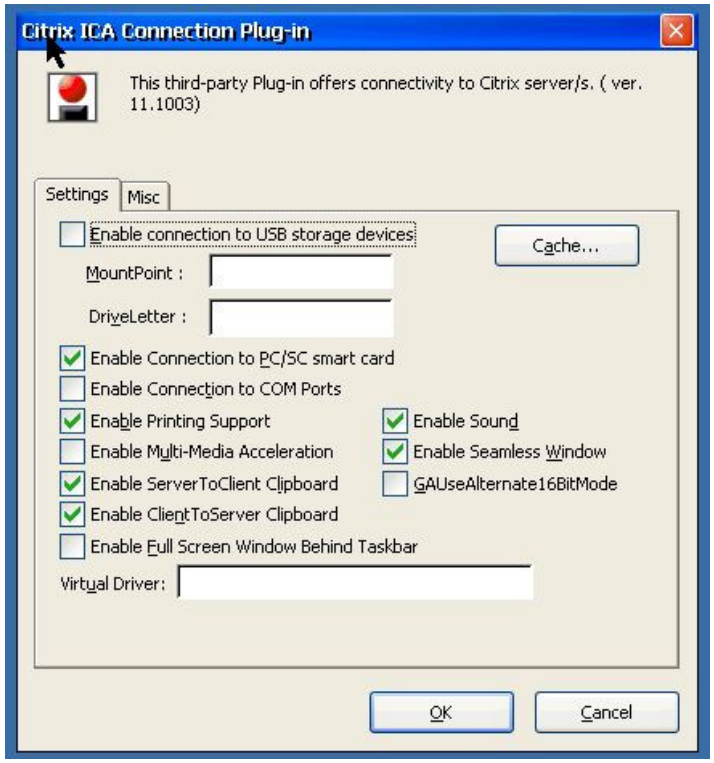
2.3 “How To” configure ICA Connection guide:

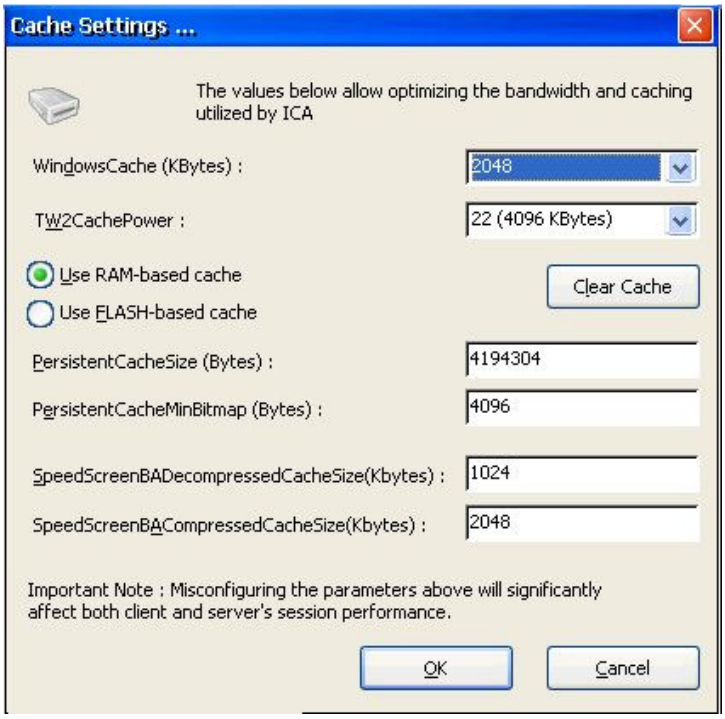
- **Configure PNAgent (server-side) settings:** PNAgent settings require both server and client side configuration. Server settings are mainly divided into two: (1) edit the default (Config.xml) file using the Program Neighborhood Administration tool (Admin tool), which provides an easy-touse graphical interface to the file's parameters. To access the PNAgent Admin tool, connect to (http://servername/Citrix/PNAgentAdmin/) on your server running the Web Interface. (2) Set additional parameters such as Application shortcuts and icon settings under the Applications interface accessible via the Citrix Farm management. (See Citrix documentation for further assistance).
- **Configure PNAgent (client-side) URL:** For PNAgent to work, client settings must point to the URL from which the Config.xml file is obtained. This is done via the ICA Plug-in \ Configure \ Misc tab by pressing the ICA Global… button, opening the Global

ICA Client Settings interface, selecting the Enable PNAgent checkbox through the Preferences tab and specifying the URL for the Web Interface server.

- **Configure PNAgent (client-side) Authentication:** PNAgent authentication varies into a number of logon methods. Assuming server side authentication is set to Prompt User; on the client, by default PNAgent proprietary 'Logon Details' window pops-up. Once providing credentials, a connection list is built according to the specified user details. In order to enable Chip PC's extension for pass-through authentication select the Use user credentials to connect to PNAgent server option located under the ICA Plug-in Configure \ Settings Tab
- **Configure Pass-through authentication in ICA connections:** Once selecting the Use user credentials for pass-through authentication option located under the ICA Plug-in \ Configure, the logged-on user credentials are automatically mapped into all ICA connections.
- **Configure PNAgent process duration:** After selecting the Enable PNAgent option, the time period to be used by PNAgent is set through the Wait for PNAgent process combo box available under the ICA Plug-in \ Configure
- **Configure PNAgent application shortcut placement & icon recognition:** Always-on, No client-side settings are needed to activate these options. Select the Use default ICA icon for PNA connections option to deactivate the icon recognition extension.
- **Auto-start PNAgent Connections:** In order to make a connection retrieved by PNAgent be auto-started perform the following: (1) Open the 'Applications' interface accessible via the 'Citrix Farm Management Consol' and select the published application you wish to auto-start. (2) Under the 'Program Neighborhood Settings' page, in the 'Program Neighborhood Folder' field type "startup" (without the quotation marks).
- **Result:** Once the devices retrieve PNAgent connections which are assigned to the "startup" 'Program Neighborhood Folder' these are automatically launched.
- **Change connection icon:** In order to change a connection's icon, select it from the connections list in the My Connections Manager, right click, select the Change Icon option and choose an icon from the built-in icons list displayed in the Change Icon window.
- **Enable smartcard mapping:** Smartcard mapping require both server and client side configuration. On the client, settings are accomplished in two levels: (1) via the ICA Plug-in properties \ Settings tab selecting the Enable connection to PC/SC smart card allows all ICA connections to use a smartcard and (2) under the ICA Connection properties \ Logon Tab select the 'Allow Smart Card logon' option.
- **Enable storage mapping:** Storage mapping require both server and client side configuration. On the client, make sure that the Enable connection to USB Storage Devices is enabled both under the USB Devices Tab of the WBT dialog as well as under the ICA Plug-in properties \ Settings tab.
- **Control Disk Caching:** Under the ICA Plug-in properties use the Cache button to define the Cache Size combo box to specify the amount of storage space (Kbytes) you would like to allocate for caching. Pressing the Clear Cache button deletes all ICA Cache contents.
- **Apply Windows Key Combination:** Under the ICA Plug-in properties \ Misc tab use the 'Apply Windows Key Combination on:' combo box to select whether to apply key combinations (e.g. ALT+TAB) locally or remotely.


Citrix ICA Connection Plug-in
This third-party Plug-in offers connectivity to Citrix server/s. (ver. 11.1003)
Settings
Misc
TransportReconnectEnabled
TransportSilentDisconnect
TransportReconnectDelay (msec):
12000
TW2StopwatchScale:
5
PrinterThreadPriority :
1
Maximize applications in Dual Screen Mode To :
Span
Use user credentials for authentication
Rules...
Use user credentials to connect to PNAgent server
ICA Global...
Use default ICA icon for PNA connections
Wait for PNAgent process (sec) :
10
OK
Cancel


Citrix ICA Connection Plug-in
This third-party Plug-in offers connectivity to Citrix server/s. (ver. 11.1003)
Settings
Misc
Enable connection to USB storage devices
Cache...
MountPoint :
DriveLetter :
Enable Connection to PC/SC smart card
Enable Connection to COM Ports
Enable Printing Support
Enable Sound
Enable Multi-Media Acceleration
Enable Seamless Window
Enable ServerToClient Clipboard
GAUseAlternate16BitMode
Enable ClientToServer Clipboard
Enable Full Screen Window Behind Taskbar
Virtual Driver:
OK
Cancel


Cache Settings ...
The values below allow optimizing the bandwidth and caching utilized by ICA
WindowsCache (KBytes) :
2048
TW2CachePower :
22 (4096 KBytes)
Use RAM-based cache
Use FLASH-based cache
Clear Cache
PersistentCacheSize (Bytes) :
4194304
PersistentCacheMinBitmap (Bytes) :
4096
SpeedScreenBADecompressedCacheSize(Kbytes) :
1024
SpeedScreenBACompressedCacheSize(Kbytes) :
2048
Important Note : Misconfiguring the parameters above will significantly affect both client and server's session performance.
OK
Cancel